NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXAMINATION OF A CAPABILITIES-BASED PRIORITIZATION SCHEME FOR SERVICE-ORIENTED ARCHITECTURE AFLOAT

by

Matthew C. Horton

September 2012

Thesis Co-Advisors:	Diana M. Angelis Gregory Miller

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Examination of a Capabilities-based Prioritization Scheme for Service-Oriented Architecture Afloat

5. FUNDING NUMBERS

6. AUTHOR(S) Matthew C. Horton

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ______N/A______.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The Navy has mandated that fielded computer systems be network-centric, service-based, and support open architectures. However, this competency is limited by network resources—namely radio frequency bandwidth—which the Navy has at its disposal. This forces decisions to be made in which some network applications take priority over others. We apply the Capabilities-based Competency Assessment process developed by Suttie and Potter to create a prioritization model for this problem of limited bandwidth. DoD Architectural Framework Version 1.5 products are used to construct an architectural description for a carrier strike-group underway, capturing each of the operational nodes working within an air detect-to-engage scenario. By linking the tasking assigned to each of these nodes and the services required for their completion, resources may be aligned to support warfare commander's intent and develop a prioritization which optimizes network performance for this tasking. Through network simulation, a comparison is made between the proposed prioritization scheme and traditional schemes. Results show our prioritization scheme consistently reduced latency and increased throughput for mission relevant applications. These improvements translate directly to more relevant information getting to decision makers at a quickened pace. Such information richness leads to "information dominance," ultimately providing superior warfighting capability.

14. SUBJECT TERMS Capabilities Based Competency Assessment, Service-Oriented Architecture, Network-Centric Warfare, Network Prioritization, Dynamic Bandwidth Allocation

15. NUMBER OF PAGES
114

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

EXAMINATION OF A CAPABILITIES-BASED PRIORITIZATION SCHEME FOR SERVICE-ORIENTED ARCHITECTURE AFLOAT

Matthew C. Horton
Lieutenant, United States Navy
B.B.A, University of Memphis, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2012

Author: Matthew C. Horton

Approved by: Diana M. Angelis
Thesis Co-Advisor

Gregory Miller
Thesis Co-Advisor

Clifford Whitcomb
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Navy has mandated that fielded computer systems be network-centric, service-based, and support open architectures. However, this competency is limited by network resources—namely radio frequency bandwidth—which the Navy has at its disposal. This forces decisions to be made in which some network applications take priority over others. We apply the Capabilities-based Competency Assessment process developed by Suttie and Potter to create a prioritization model for this problem of limited bandwidth. DoD Architectural Framework Version 1.5 products are used to construct an architectural description for a carrier strike-group underway, capturing each of the operational nodes working within an air detect-to-engage scenario. By linking the tasking assigned to each of these nodes and the services required for their completion, resources may be aligned to support warfare commander's intent and develop a prioritization which optimizes network performance for this tasking. Through network simulation, a comparison is made between the proposed prioritization scheme and traditional schemes. Results show our prioritization scheme consistently reduced latency and increased throughput for mission relevant applications. These improvements translate directly to more relevant information getting to decision makers at a quickened pace. Such information richness leads to "information dominance," ultimately providing superior warfighting capability.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAWC	Anti-Air Warfare Coordinator
ADC	Air Defense Commander
ADNS	Automated Digital Network System
AIC	Air Intercept Controller
BB	Bravo Bravo (Carrier Strike Group Commander)
BQ	Bravo Quebec (Command and Control Warfare Commander)
BW	Bravo Whiskey (Air Warfare Commander)
C2W	Command and Control Warfare
C4I	Command, Control, Communications, Computers, and Intelligence
CAC	Call Admission Control
CANES	Consolidated Afloat Networks and Enterprise Services
CBCA	Capabilities-based Competency Assessment
CBWFQ	Classed Based Weighted Fair Queuing
CBQ	Classed Based Queuing
CENTRIXS-M	Combined Enterprise Regional Information Exchange System – Maritime
CG	Guided Missile Cruiser
CIEA	Classification, Identification, and Engagement Area
CO	Commanding Officer
COI	Community of Interest
COPS	Common Open Policy Service
CPU	Central Processing Unit
CRUDES	Cruiser/Destroyer
CSC	Combat Systems Coordinator
CSG	Carrier Strike Group
CVN	Aircraft Carrier, Nuclear Powered
CWC	Composite Warfare Concept
CWSP	Commercial Wideband Satellite Program
DCA	Defensive Counter Air
DDG	Guided Missile Destroyer

DIFFSERV	Differentiated Services
DIFFSERV-TE	Differentiated Service Traffic Engineering
DoD	Department of Defense
DON	Department of the Navy
DODAF	Department of Defense Architectural Framework
DSCP	Differentiated Service Code Point
DRE	Mission-Critical Distributed, Real-Time, Embedded
DTE	Detect-to-Engage
EHF	Extremely High Frequency
EW	Electronic Warfare
EWC	Electronic Warfare Coordinator
FIFO	First In, First Out
FOTC	Force Over The Horizon Track Coordinator
GENSER	General Service
GIG	Global Information Grid
HVU	High Value Unit
INMARSAT	International Maritime Satellite Program
INTSERV	Integrated Services
IP	Internet Protocol
ISNS	Integrated Shipboard Network System
ISP	Internet Service Provider
LAN	Local Area Network
METL	Mission Essential Task List
MMHS	Military Message Handling Systems
MSS	Missile Systems Supervisor
NATO	North Atlantic Treaty Organization
NCF	Naval Cyber Forces
NCW	Net-Centric Warfare
NEC	Network-enabled Capabilities
NFFI	North Atlantic Treaty Organization Friendly-Force Information
NTA	Navy Tactical Task
OPTASK	Operational Tasking

OV-2	Operational Node Connectivity Description
OV-4	Organizational Relationships Chart
OV-5	Operational Activity Model Description
PEO C4I	Program Executive Office for Command, Control, Communications, Computers and Intelligence
PMW	Program Manager, Warfare
PPR	Pre-planned Response
QED	Quality of Service-Enabled Dissemination
QRG	Quality of Service-Aware Residential Gateway
QOS	Quality of Service
RED	Random Early Detection
RF	Radio Frequency
RSC	Radar Systems Coordinator
RSVP	Resource Reservation Protocol
SA	Surveillance Area
SCI	Sensitive Compartmented Information
SHF	Super High Frequency
SOA	Service-Oriented Architecture
SV-4	Systems Functionality Description
SV-5A	Operational Activity to Systems Function Traceability Matrix
TAO	Tactical Action Officer
TADL	Tactical Data Link
TDM	Time Domain Multiplexing
TIC	Track Information Coordinator
TOS	Type of Service
UDP	User Datagram Protocol
UNTL	Universal Naval Task List
VA	Vital Area
VOIP	Voice Over Internet Protocol
WRED	Weighted Random Early Detection
XML	Extensible Markup Language

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The United States Navy has put forth a mandate for fielded computer systems to be network-centric, service-based, and support open architectures. The purpose for this move is to gain an increase in combat effectiveness through the networking of the warfighter while at the same time building in the flexibility to easily modify and expand the existing network architecture. By leveraging this capability, the Navy can field a rapid, adaptable, war-fighting network, easily tailored to the task at hand. However, this competency is still limited by the network resources—namely radio frequency (RF) communications systems bandwidth—which the Navy has at its disposal (PEO C4I, 2011). This limitation of resources forces decisions to be made in which some network applications must take priority over others. This decision-making requirement led to the two questions around which this report is focused:

> 1) What is the feasibility of developing a bandwidth utilization priority scheme based upon identified tasks and information required by warfighters to conduct military operations within a hostile environment?
>
> 2) How will this systematic allocation process, based upon warfighter information needs and dynamically tailored for various threats, affect data latency and information throughput?

In order to correctly prioritize Navy tactical networks to meet the need of the warfighter, we must leverage network Quality of Service (QoS) provisions tailored to DoD needs. Managing QoS allows system administrators to tailor network resources and prioritization to match what the user needs. The Navy currently deploys the Automated Digital Network System (ADNS) – Increment III to manage the transmission and prioritization of Internet Protocol (IP) – based network traffic. While ADNS does implement QoS management, it was not designed with the needs of the warfighter as its primary focus nor does it provide the capability to dynamically manage network priority based on changing threats.

We propose to optimize warfighter abilities by matching network system priorities to the prioritization of the tasks required to accomplish the overarching warfare capability. Central to our approach is an understanding of how the U.S. Navy wages war at sea. Our process leverages current surface warfare doctrine and encompasses the Composite Warfare Concept (CWC) employed by surface units operating at sea. We use a carrier strike group (CSG) to illustrate our process as the CSG is and will continue to be the cornerstone of U.S. Naval strategy. Air defense operations being carried out by the CSG are used because few other warfare areas pose the unique challenges of sea-based air defense—perhaps chief among them being the need for rapid, networked response.

This study follows the Capability-Based Competency Assessment approach developed by Suttie & Potter (2008), to identify Mission Essential Task Lists (METLs). The METLs are used to identify a set of competencies which incorporate operations, personnel, and system requirement inherent to air defense operations. We start by using the Department of Defense Architectural Framework (DoDAF) Version 1.5 products to capture the roles and responsibilities of each of the individuals who make up a ship's air defense team. These individuals act as operational nodes upon which the strike group's functional architecture is built. An Organizational Relationships Chart (OV-4) is used to clarify these roles and to clearly delineate the operational hierarchy. Next, we use an Operational Node Connectivity (OV-2) diagram to capture the actual structure of those individuals working within the strike group. The OV-2 shows the lines of communication and information flow between each of the operational nodes. Each of these operational nodes is assigned tasking which, when completed, aggregate to complete the overarching task of executing air defense operations.

This tasking is identified using the Universal Naval Task List (UNTL). The UNTL serves as a repository for tasks that can be completed by Naval forces. These tasks are considered essential for mission accomplishment (Chief of Naval Operations, Commandant, United States Marine Corp, Commandant, United States Coast Guard, 2007). By parsing this list of mission capabilities and identifying the relevant mission tasks, we develop the METLs suggested by Suttie and Potter and prioritize tasks based on their relevance to the mission at hand. Using an Operational Activity Model (OV-5), each of these tasks is assigned to the operational node responsible for their completion and their relevance to one another is made clear. Next, we seek to identify those network systems which are relevant to this mission tasking.

The Command, Control, Communications, Computers, and Intelligence (C4I) Masterplan serves to summarize the major attributes of DoN network-centric systems. It provides baseline descriptions of the networked systems fielded by the Navy and identifies the platforms to which they are assigned (PEO C4I, 2011). Using the system descriptions presented in the C4I Masterplan, a list is developed of those systems required to conduct air defense operations. By using a System Functionality Description (SV-4a) viewpoint it is possible to break down each of the relevant, net-centric systems and identify their provided functionality. The relationships between those systems are mapped, thus providing the structure of the viewpoint.

The DoD guidance on *Architectural Framework Version 1.5, volume II,* defines an Operational Activity to Systems Function Traceability Matrix (SV-5a) as documenting the relationship between the operational activities and system functionality present in the overall architecture. It is this relationship that is most beneficial for the purpose of this thesis. By linking the operational nodes which are passing information to the corresponding data relationships captured by a SV-5a, the form of the service-oriented architecture takes place. The resulting prioritization scheme aligns operational nodes and services within the overall system architecture so that commanders are able to more effectively use existing network resources to accomplish required tasks within a compressed time frame. By linking the identified systems to the application types ADNS recognizes, we have provided mission specific justification for the prioritization of one network application over another, thus answering to the first of our two questions.

To answer the second question, we developed a simulation model that captures the current Navy data processing environment. The model is used to compare our prioritization scheme to current network prioritization templates in the context of an air detect-to-engage scenario. The results show that our prioritization scheme consistently reduced latency and increased throughput for mission relevant network applications as compared to current network prioritization schemes. These improvements were both statistically and practically significant. Decreases in latency and increases in throughput translate directly to more relevant information getting to decision makers at a quickened pace. Such information richness leads to “information dominance,” ultimately providing superior warfighting capability.

The steps developed in this thesis are designed to be used by tactical commanders during the planning process prior to a strike group’s workups. This thesis provides a detailed architectural model which may be used to align warfare commander’s priority and intent with existing network capabilities and provides a common tool for communicating warfare commander’s intent to those responsible for carrying out that intent. This approach should be used to help Navy networks achieve the warfighting capacity for which they were designed.

ACKNOWLEDGMENTS

I would like to take this opportunity to extend my most sincere thanks to my thesis advisors, Dr. Diana Angelis and Prof. Gregory Miller. Without their patient guidance and insightful feedback, this work would not have been possible. I would also like to thank Dr. Weilian Su and Prof. Mary Vizzini for their helpful comments and advice. To the countless others who have provided insight, clarification, and avenues for improvement I offer a heartfelt “thank you.” Finally, to Ginger: Thank you for being my anchor. Without you I would have long ago been led astray.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I) Masterplan serves as a repository of information for all Navy and many Joint network-centric applications (PEO C4I, 2011). It acts to summarize the major programs of the Department of the Navy (DoN) as applicable to network operations, providing outlines of planned future capabilities, their major characteristics, and timelines for their implementation. The main purpose of this documentation is to "improve the unified focus across the PEO C4I enterprise in order to provide Navy and Joint warfighters with the best network-centric information dominance capabilities that fully support their missions" (PEO C4I, 2011).

To support this focus, the PEO C4I Masterplan has put forth a mandate for fielded computer systems to be network-centric, service-based, and support open architectures. The purpose for this move is to gain an increase in combat effectiveness through the networking of the warfighter while at the same time building in the flexibility to easily modify and expand the existing network architecture. By leveraging this capability, the Navy can field a rapid, adaptable war-fighting network, easily tailored to the task at hand. However, this competency is still limited by the network resources—namely radio frequency (RF) communications systems bandwidth—which the Navy has at its disposal (PEO C4I, 2011). This limitation of resources forces decisions to be made in which some network applications must take priority over others. This suggests two research questions that will be explored in this thesis: (1) "What is the feasibility of developing a bandwidth utilization priority scheme based upon identified tasks and information required by warfighters to conduct military operations within a hostile environment? And (2) "How will this systematic allocation process, based upon warfighter information needs and dynamically tailored for various threats, affect data latency and information throughput?"

To answer the research questions we must first gain an understanding of the needs of the warfighter—the thought processes and the tactics used in the battlefield. The centerpiece for U.S. Naval strategy is the carrier strike group (CSG). The carriers themselves are dynamic platforms equipped with a wide variety of assets which may be used both tactically in war as well as for more peaceful missions. These assets are coupled with escort vessels equipped with the best and most modern sensors and weapons fielded for battle at sea, each of them manned by technically proficient crews capable of not only naval combat but also disaster relief. This inherent flexibility makes the aircraft carrier not only suited for war but also as an instrument for peace. Any naval network prioritization scheme designed without taking the needs and the operating practices of the CSG into account will have been developed in vain. It is also critical that we define the doctrine the Navy uses to provide command and control at sea. Using this doctrine as our foundation, we can build the framework for our prioritization scheme by capturing the operational relationships and functional architecture of both the systems and the operators working within the CSG.

The Department of Defense Architectural Framework (DoDAF) is the guiding document for the development of such functional architectures. It provides a standardized format and set of rules for the representation and comparison of DoD architectures (DoD, 2007). This guidance continues to evolve as the definitions of what comprises architecture develop and as the DoD makes moves to encompass NCW. DoDAF Version 1.5 has been uniquely tailored to the needs of the net-centric environment.[1] It has as its focus those net-centric concepts that are shaping the way the DoD wages war and it allows for the development of architectural artifacts which describe mission operations and processes and those operational activities responsible for their completion (DoD, 2007). Additionally, DoDAF Version 1.5 encompasses those systems utilized by identified operational activities to complete mission tasking. The benefit of using DoDAF to represent the CSG is that it provides a succinct representation of the operators and systems working within its architectural framework. It captures the relationships between the system operators working in this environment and allows an observer to understand

[1] Although DoDAF Version 2.0 has been published, it defines systems as encompassing not only hardware and software but also those non-machine components, i.e., human operators, with which the system interacts (DoD, 2009). The nature of the approach to be defined in this paper requires specific delineation between computer systems and the operators which use them. For this reason, DoDAF Version 1.5 will be used for all architectural descriptions.

the information relationships required to complete operational tasking. Once these relationships have been correctly identified, it is then possible to develop a methodology for their correct prioritization.

Having gained an understanding of how the Navy makes war, it is then critical to comprehend the methods and technologies implemented to manage its tactical networks. The Navy currently deploys the Automated Digital Network System (ADNS)–Increment III to manage the transmission and prioritization of Internet Protocol (IP)–based network traffic. The ADNS and Tactical Networks Program offices have fielded documentation which describes the usage of ADNS and how it manages network behavior (Automated Digital Network System, 2011). This document describes the process by which ADNS marks network traffic, based on class discrimination, and the queuing behavior by which it prioritizes the traffic which it transmits. The current network prioritization scheme implemented on ADNS does not rank applications based on their use by the warfighter in a combat environment but rather seeks to optimize network performance based on application characteristics. While this approach may work for a civilian, bandwidth rich environment, it does not fully support the main purpose of Navy tactical networks, i.e., war fighting.

In order to correctly prioritize Navy tactical networks to meet the need of the warfighter, we must leverage network Quality of Service (QoS) provisions tailored to DoD needs. The PEO C4I Masterplan defines QoS as “the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow” (PEO C4I, 2011). Managing QoS allows system administrators to tailor network resources and prioritization to match what the user needs. The need for network QoS management was born from the increasing diversity and capability of modern computer networks. As more and different network applications have been developed, the need to manage their different network resource requirements has evolved. As the robustness of these applications increases, so too must the ability to manage them. While ADNS does implement QoS management, it was not designed with the needs of the warfighter as its primary focus nor does it provide the capability to dynamically manage network priority based on changing threats. Therefore, it is prudent to consider additional QoS management approaches. There are two generally accepted methods of implementing network QoS management: Integrated Services and Differentiated Services.

A. INTEGRATED SERVICES

Integrated Services (IntServ) works by providing bandwidth guarantees to network applications, given that the routers between the source and destination applications support IntServ capability (White, 1997). This is opposed to “best-effort” traffic flows which receive no guarantee and will only be provided those network resources that are available. This “reservation” of network resources is accomplished by network management or via the Resource Reservation Protocol (RSVP) network protocol in which each network router works to request the needed network resources prior to transmission (White, 1997). Assuming the network request is accepted, the required network resources are reserved for the session between the applications requesting the bandwidth commitments.

Wang et al. (2004) have proposed an IntServ technique utilizing the publish/subscribe style. Their proposal requires service requesters to develop and transmit QoS messages (utilizing an Extensible Markup Language (XML) based QoS language) to network service providers. XML is a “user-friendly” computer language designed to be readable by both the machines running the instructions and the humans controlling those machines. These messages are used to define the requested QoS characteristics and to develop QoS contracts which are used to parse out available network resources to the requesting application. Their approach utilizes ten separate network services to implement, monitor, and manage network QoS at the middleware layer (Wang et al., 2004)—middleware layer being software designed to provide resources to applications separate from that which the operating system provides. They demonstrated through experimentation the effectiveness of their technique in reducing end-to-end delays and the provision of responsive QoS to varied client requirements.

Integrated services are somewhat difficult to implement and, as a result, limited research has been conducted regarding its implementation in QoS management; nevertheless it should be recognized as a potential solution for tailoring DoD QoS implementation.

B. DIFFERENTIATED SERVICE

The Differentiated Services (DiffServ) model works by taking advantage of the Type of Service (TOS) byte within the Internet Protocol Version 4 (IPv4) header (Xiao & Ni, 1999). By manipulating three bits within this byte, applications may specify requirements for the handling of their associated data. Like type services may be grouped together and a set of rules derived for the handling of each particular data type—also known as an aggregate class. Although DiffServ is not as readily tailored to specific network applications as IntServ, its generality makes it far easier to implement and, as a result, it has a much wider application as a QoS management tool in networks (Xiao & Ni, 1999). One disadvantage to DiffServ is that it is only as effective as the level of granularity that the client's Internet Service Provider (ISP) allows. The level of control available in DiffServ is achieved through service level agreements that are negotiated between the client and the ISP beforehand.

Given the Navy is its own ISP, there is a level of control not present for most Internet consumers, but formalized rules for QoS management must be in place for both deployed units and the operating center through which that unit connects to the Internet at large. Theses rule sets would need to be coordinated beforehand so that when the time comes to implement them they may be done so without error. The Navy currently utilizes an adaptation of the DiffServ model to implement QoS management (Automated Digital Network System, 2011).

One approach to QoS management which is very similar to the capabilities of ADNS is the work conducted at the University of Florence in Florence, Italy. Ronga et al. (2003) have proposed an integrated management QoS management scheme which incorporates DiffServ capability coupled with a resource management scheme for providing QoS to aggregated end users connecting to the Internet via satellite. Their proposal utilizes three major components: traffic marking—which makes use of the IPv4 Type of Service (TOS) field to mark traffic, priority management—which incorporates random early detection (RED) and First in, First Out (FIFO) policies to meet short term QoS requirements, and dynamic resource management—which performs long term bandwidth reservation to balance resource allocation (Ronga et al., 2003). ADNS incorporates a policy known as weighted random early detection (WRED) in which separate traffic classes are given weights based upon their level of importance. This weighting provides for a lower probability that a particular traffic type will be dropped instead of transmitted, based on the level of information present on the network. ADNS behavior will be explored in more depth in Chapter VI. Through experimentation, Ronga et al. demonstrated the effectiveness of their approach in providing adequate resource allocation for short term traffic bursts while maintaining balanced data throughput across the various application types.

C. DYNAMIC BANDWIDTH ALLOCATION

The previously described applications work well if the need of the network is static; however, the threats posed against Navy units are dynamic and fluid. Leaders must often adapt strategies and weapons systems to meet the challenge they are currently facing. Given this fact, Navy networks must possess the ability to be changed by the operators they are designed to support. Dynamic bandwidth allocation is a process by which available network resources, namely bandwidth, are shared fairly among all users on that particular network. It takes advantage of the fact that most network traffic is not constant and that there is natural variability in the amount of bandwidth required by any user at any given time. This network traffic behavior is classified as being "bursty," meaning there are often significant gaps between transmissions by a single application; during those gaps, network resources may be given up to other applications requiring them. Dynamic bandwidth allocation is implemented through the process of packet-based transport. One challenge to this is the dynamic tailoring of QoS management is still in its infancy, namely, changes to the client's desired QoS settings require matching changes be implemented on the service provider side, making rapid tailoring of network priorities difficult to implement.

One area of research that shows potential is being conducted by IEEE members Wen-Shyang Hwang and Pei-Chen Tseng. Hwang and Tseng (2005) have proposed the development of what they call a QoS-aware Residential Gateway (QRG). While tailored for the residential-based network, their QRG approach provides insight into possible methods for increased user-friendly network control. QRG works by directed network traffic flows to defined classes via the DiffServ model. These classes may be prioritized for transmission, thus allowing precedence to be given to high priority traffic. Their approach also incorporates classed based queuing (CBQ) to provide for tighter management of network resources. They have incorporated an auto-configuration feature which allows, via a user friendly interface, the ability to select network settings based on either two preset configurations or allowing the user to manually configure the network settings, including RSVP and DiffServ settings. Through experimentation, they demonstrated significant improvement in data throughput for defined user applications as opposed to default network settings without DiffServ controls. Their approach seeks to incorporate user network control without negative impact to other users on the same wide area network. With further research, it possible that their methodology could be employed on a larger scale, thus allowing finer control of network QoS management at the unit level. This approach would greatly simplify user interaction with the QoS management application allowing greater flexibility and more rapid response to changing threat conditions as required for Naval applications.

Other useful research is being conducted by Stefano Salsano of the University of Rome and Luca Veltri of the Italian Research Consortium on Telecommunications. Salsano and Veltri (2002) have proposed utilizing and extending the Common Open Policy Service (COPS) protocol to transfer information relating to network resource allocation between servers and clients. COPS is a subset of the Internet Protocol and works as a set of business rules for the implementation of QoS. It serves as a liaison between the systems enforcing network policies and those which make decisions regarding network policy (Salsano & Veltri, 2002). They suggest its usage in the interface between edge nodes and resource allocation nodes to facilitate dynamic QoS management in a DiffServ network. This model should allow for provision of network resources to local nodes, ease of local node requests to resource providers and the capability to handle specific network requests. These network requests would include information about the amount of resources requested, the type of services required, and to which queues the resource requests applies. They argue their approach leads to a possible method for implementation of dynamic DiffServ QoS as opposed to a static prioritization scheme. Application of their research could lead to a more streamlined process by which the Navy could implement dynamic QoS management, simplifying the resource allocation process and providing greater network control.

To gain an understanding of how QoS provisions manage network traffic, it is important to explain how information routing is conducted in modern network infrastructures. There are two approaches for transporting information along a network: packet-based transport and time domain multiplexing (TDM). TDM offers the benefit of dedicated lines of pathways of communication between end-users facilitated by timesharing of network pathways. Packet-based transportation divides data streams into manageable data blocks known as "packets," which are then transported along the network via header information contained within each packet. While more conducive to QoS management, TDM suffers compared to packet-based transportation methods in terms of cost effectiveness. This difference has caused many network services to move away from the legacy TDM infrastructure towards packet-based services (Kashihara & Tsurusawa, 2010).

Kashihara and Tsurusawa further indicate that QoS management within a packet-based IP network is more difficult to implement, requiring a pathway with sufficient, guaranteed bandwidth and traffic flows managed to not exceed that bandwidth guarantee. Networks which leverage these kind of controls have already been proposed—incorporating DiffServ traffic engineering (DiffServ-TE) protocols for core routers and Call Admission Control (CAC) for edge routing (Kashihara & Tsurusawa, 2010). We have previously described the capabilities of the DiffServ model. CAC works by monitoring and adjusting IP flow between source and destination clients based on traffic demand. Kashihara and Tsurusawa have proposed a technological solution that seamlessly integrates the dynamic management of both core and edge bandwidth allocation. Their methodology incorporates regular monitoring of edge router traffic flows which aggregate to the total demand on the core router. As traffic requirements increase at the edge, the core router looks to expand its available pathway for transmission. If these required resources are not available, the edge routers implement CAC controls to reject inbound network traffic and reduce the overall demand on the network (Kashihara & Tsurusawa, 2010). Through experimentation, they were able to demonstrate the effectiveness of their methodology in the estimation of required bandwidth by up to 800 flows to within 99.9% accuracy. Their approach provides a more accurate prediction of the amount of resources a particular dataflow requires than default best-effort processing. Utilizing this predictive approach, it is possible to supply applications with only the resources they require and no more. Doing so frees up bandwidth to be applied elsewhere and maximizes the network resources at hand. This is particularly relevant to the Navy, given that bandwidth at sea comes at a premium.

Zhao et al. have proposed a methodology which seeks to balance the rate of packet loss for different classes of network traffic working within the DiffServ model. Traditionally, bandwidth allocation to separate aggregate classes within DiffServ is static. This has led to mismatches between assigned bandwidth and network demand, thus prompting work in dynamic bandwidth allocation. They indicate that one approach that has been developed to dynamically assign bandwidth, namely methods which utilize traffic characteristics, i.e., the number of packets in each aggregate class, has fallen short in its implementation (Zhao et al., 2012). This flow-number method only incorporates the number of packets and not the size of each these packets, possibly leading to increased packet loss. They propose a method which incorporates not only the number of packets assigned to each aggregate class but also the size of those packets. Through experimentation, they were able to demonstrate a marked improvement in the balance of packet loss between aggregate classes using their methodology as opposed to traditional flow-number approaches.

The methods and technologies we have presented here are by no means comprehensive, but they do provide a fairly wide sampling of potential solutions for the implementation of QoS management. In addition, they highlight efforts being conducted within the civilian sector that are applicable to military networks. Having now gained an understanding of the state of network QoS technology, it is important to consider how the Navy's net-centric architecture is deployed.

D. SERVICE-ORIENTED ARCHITECTURE

Recall the PEO C4I Masterplan's mandate for service-oriented, open architectures. Lund et al. (2007) of the Norwegian Defence Research Establishment define Service-Oriented Architecture (SOA) in the military context as "a way of making military resources available as services so they can be discovered and used by other entities that need not be aware of those services in advance." They have conducted extensive research into the applicability of SOA in the implementation of military communication networks. They note the benefits of such an approach in providing access to military resources across the spectrum of military operations, including coalition and unilateral actions. They highlight a North Atlantic Treaty Organization (NATO) study into network-enabled capabilities (NEC) which was conducted to develop a cooperative strategy for development of network enabled systems across coalition networks (Bartolomasi et al., 2005). The study emphasizes the need for any such systems to enable shared situational awareness and to provide QoS capability. Lund et al. note the issues with developing SOA for military use; primarily that SOA was initially developed for use in a bandwidth rich environment. They describe this as being equal to military applications at the strategic level, but highlight that for SOA to be truly effective it must also incorporate units at the tactical level. This requirement is unique in that many units operating at this level are extremely limited in their connectivity. Lund et al. call this condition "a disadvantaged grid." They note several approaches for enabling SOA in a military environment including general compression of XML and the use of binary XML. Through experimentation, they demonstrated the effectiveness of both approaches in providing significant reduction in network traffic. They further indicate the importance of streamlining the data exchange process. They recommend a hybrid approach in which deployed databases are synchronized using a push-based exchange of NATO friendly-force information (NFFI)-messages. This approach assumes the implementation XML compression and binary XML to reduce the data present on the network. They go on to describe methods for implementing communication across the heterogeneous infrastructure of which coalition networks are often comprised. Their approach leverages the already existing standard for military message handling systems (MMHS) to implement store-and-forward processes for data transfer. Finally, they touch on the importance of QoS in this SOA environment. They state that even with their approaches in place, data requirements may still exceed the resources available. As a result, some form of QoS management must be implemented for SOA to be truly effective for military use.

Loyall et al. (2012) have noted some shortfalls of SOA in the provision of QoS. They note this gap becomes evident in the lack of its adoption in mission-critical distributed, real-time, and embedded (DRE) domains, due to their demanding performance requirements. They argue that many of the conventions which make SOA desirable, namely flexibility and scalability, also make it less effective for those systems requiring greater control and QoS management. They have proposed four separate services and mechanisms to implement what they call QoS-Enabled Dissemination (QED). Their method incorporates an aggregate QoS management service—which works to develop policies for all local QoS management systems and maintain predictable network behavior, a QoS policy service—maintaining those policies set by the QoS management system, a task management local QoS manager—designed to manage and execute central processing unit (CPU) intensive operations for each client, and a bandwidth manager—providing bandwidth based on the policies set by the QoS management system. Through experimentation, they demonstrated the effectiveness of the QED process in improving the effectiveness of existing SOA middleware in implementing QoS management in a DRE environment.

Having gained an understanding of SOA and its context for military applications, we next look for a relationship between SOA and the architectural structure we will define for the CSG. Doing so allows us to truly prioritize those systems which are the most important relevant to a given mission. Using the technologies we have previously described, it is then possible to deploy a network prioritization scheme which emphasizes the user’s needs.

E. CAPABILITY-BASED COMPETENCY ASSESSMENT

Recent efforts by the Naval War College have developed a high level architecture for maritime operations based on a concept of globally linked Maritime Operations Centers. Through the process of Capability-Based Competency Assessment (CBCA), mission essential tasks have been identified and translated into a set of competencies which incorporate operations, personnel, and system requirements. These competencies act as operational nodes on which the high level architecture is developed. We can leverage their methodology, which seeks to map task to operator, and operator to system, to develop our architectural framework for true war-fighting optimization. Defining such architecture is a crucial first step in understanding the impact of SOA and capturing the benefits of its deployment. The end goal of this high level architecture is to improve command and control and aid the decision maker at the enterprise level. Operating at this level of abstraction, it is imperative that the architecture capture not only the people or processes to be implemented, but also the links between the processes as well as the information required and the methods for completing those processes. By identifying these operational nodes and linking them to the network services required for completing their assigned tasks, a service-oriented architectural description for Navy battle groups underway may be developed.

Such an approach departs from the traditional, billet-based, allocation of personnel and seeks to define "roles" which act as critical nodes that correspond to a DoDAF Operational Node Connectivity Description (OV-2) of the overall operational architecture. These roles would act independently of the personnel assigned to complete them; however, training pipelines would ideally be tailored to fill those roles. Through the process of CBCA, these roles, and their associated subtasks—i.e., processes—may be identified and the duration and prioritization of each of those subtasks determined. By linking the operational nodes which are passing information to the corresponding data relationships captured by an Operational Activity to Systems Function Traceability Matrix (SV-5a), the form of the SOA may begin to take place. Operational nodes and services are better aligned within the overall system architecture and commanders are able to more effectively use existing network resources to accomplish required tasks within a compressed time frame.

By using the relationships identified in our SV-5a viewpoint, we can recognize those systems which are most relevant to the threat at hand and give them precedence over other networked systems operating on the network. These relationships are mission-oriented and provide the justification necessary for preferring one network application over another. This preference is done by separately classifying those relevant systems and assigning sufficient bandwidth to them in order to achieve a desired outcome—i.e., ensuring latency and throughput are within an acceptable level. Once we have developed our proposed prioritization scheme, it will be tested and compared to the existing ADNS prioritization scheme in a scenario designed to stress the networks of both the aircraft carrier and its escort vessels. We will use the results for comparison and analysis and draw conclusions from the information we gather.

The end goal of this approach is to provide a clear process for the prioritization of network traffic which can be manipulated and expressed by both the tactician and the technician. Rather than expressly dictating the actual networked systems which should take priority over others, we have sought to develop a methodology by which the commander, who may not be well versed in computer science, can sit down with those operating his networks and develop a prioritization scheme that optimizes his computer networks as a weapon. Too often, Navy shipboard networks are seen simply as administrative systems and that become a burden when they do not operate properly. As the Navy transitions to a truly networked architecture, so too must our commanders evolve to capture the benefits that such a networked approach brings. Ideally the process we outline here would be used in conjunction with the Operational Tasking (OPTASK) orders that are already defined for a strike group prior to sail and the centralized planning process that occurs during the warfare commander’s conference. As the level of threat to his ships increases, the network may be shifted to provide optimum capability against the threat-at-hand. The strike group commander would define those systems which are most relevant to the particular mission at hand and would prepare a set of pre-planned responses (PPRs) for the operation of the networks, just as he would for any other weapon system at his disposal. Only when we begin to think of our computer systems as weapons of war may we truly optimize them for that purpose.

In this paper, we will look at two research questions:

> 1) What is the feasibility of developing a bandwidth utilization priority scheme based upon identified tasks and information required by warfighters to conduct military operations within a hostile environment?
>
> 2) How will this systematic allocation process, based upon warfighter information needs and dynamically tailored for various threats, affect data latency and information throughput?

To answer the first question we will propose a methodology which seeks to prioritize network applications based upon their relevance to the warfighter. We will outline a process—which links task to operator and operator to system—for developing such a prioritization scheme and demonstrate its effectiveness in limiting relevant data latency and increasing relevant data throughput. In so doing, we will seek to get the most pertinent information to decision makers faster, thereby yielding superior tactical network usage.

To answer the second question we will develop a realistic, wartime scenario in which to vet the effectiveness of our prioritization scheme and compare its results with that of existing Navy network prioritization schemes. Finally, using the results from our scenario, we will draw conclusions regarding our methodology’s effectiveness and make recommendations for future research and implementation.

II. STRIKE GROUP FUNCTIONAL ARCHITECTURE DESCRIPTION

A. CURRENT SURFACE WARFARE DOCTRINE

Our prioritization scheme is designed to optimize warfighter abilities by matching network system priorities to the prioritization of the tasks required to accomplish the overarching warfare capability. In order to develop our prioritization methodology, we must gain an understanding of the functional architecture for which the network in question is designed to support. Doing so allows us to capture the relationships between the warfighters operating in this system-of-systems and will ultimately provide the justification for our prioritization scheme. The first step in this process is to define the scope of the system-of-systems we will be examining. For the purpose of our study, we will be examining the impact of our prioritization scheme on the Carrier Strike Group. The following section explains the prominence the aircraft carrier holds in American foreign policy and why we choose it to vet our methodology.

1. The Importance of the Carrier Strike Group

The President's strategic guidance details America's ability as the sole nation capable of military power projection and sustained military operations. As a country, we retain the right to use force when necessary and extend our control when all other means of coercion have been exhausted. Included in this sphere of control is the ability to ensure the constant flow of commerce by keeping the sea lanes open for safe transit (Office of the President of the United States, 2010).

Prerequisite to exercising this control is a strong naval force that acts as the arm of its home nation. Alfred Thayer Mahan (1890) argued that the very existence of the Navy is due to the need to protect the commercial interests of its country. Because of the global nature of American interests, it follows that the United States must be able to employ power on the sea.

Dr. Daniel Goure of the Lexington Institute indicates that the Carrier Strike Group (CSG) is the essence of this naval power for the United States. He states that the CSG is "able to exert influence and control over an enormous volume of sea and air space, ensuring the free flow of goods and people across the global commons." Additionally, he argues that the destructive power a CSG can levy against hostile forces is unparalleled in conventional warfare (Goure, 2011). Given the unmatched benefits, the CSG will continue to serve as the primary instrument of U.S. force projection well into the 21st century (PEO C4I, 2010). For this reason, the CSG will serve as the principle subject of this thesis.

2. Composition of the Carrier Strike Group

There is no formal definition of a CSG (United States Navy, 2012). The formation and composition of a CSG are variable depending on the circumstances of its use; however according to the U.S. Navy's website, a CSG is typically comprised of the following:

- An aircraft carrier—an aircraft carrier is a large deck ship, over 1,000 feet in length, and equipped with 60+ aircraft capable of extended on-station time and a wide variety of missions. Nuclear powered, the aircraft carrier is capable of extended operations at high speed and is an integral part of U.S. strategy abroad. The aircraft carrier serves many roles for the United States. These include U.S. power projection and humanitarian aid. In this capacity, the carrier serves as the high value unit (HVU) around which the other units within the strike group are centered. In addition, the carrier also houses the strike group commander and the majority of his staff. As such, the carrier is the central hub around which the strike group is built.
- A guided missile cruiser—the *Ticonderoga* class guided missile cruiser is a gas turbine warship with a crew of over 350 personnel. Equipped with the AEGIS combat suite and a wide variety of missile and gun systems, the guided missile cruiser is well equipped in its primary role of air defense. The AEGIS combat suite is an integrated sensor and weapons systems using the SPY-1 phased array radar, weapons control computers, and the vertical launch system for anti-air missile deployment. The guided missile cruiser typically serves as the air defense commander (ADC) and is responsible for the coordination of area air defense around the strike group.
- Two guided missile destroyers—the *Arleigh Burke* class guided missile destroyer is an AEGIS, gas turbine warship armed with air, surface and subsurface weaponry. The guided missile destroyer is capable of a wide variety of missions and is considered one of the most powerful warships ever fielded. In the CSG, the guided missile destroyers serve in a primarily air defense role.

- An attack submarine—the *Los Angeles* class attack submarine serves as the backbone of the U.S. submarine force. While many are capable of launching the Tomahawk cruise missile, the *Los Angeles* class is primarily employed to seek out and destroy enemy submarines and surface combatants. As such, the attack submarine serves to defeat surface and sub-surface threats to the CSG.
- A logistic support ship—the *Supply* class is a high speed vessel capable of extended operations alongside the CSG. Operating under the Military Sealift Command, the logistic support ship provides support to the other ships within the strike group and is capable of carrying more than 170,000 barrels of oil and a wide variety of provisions and ammunition.

Each ship type plays a vital role in the operation of the CSG, and although there is no standardized CSG format, this grouping is typical and will be considered the composition for analysis. In an air defense scenario, the purpose of the ships other than the carrier in the strike group is to offer defensive support for and enable the HVU.

Milan Vego (2007) of the Naval War College classifies this defensive support as *operational protection*, the goal of which is "to protect the physical capabilities and moral strength of one's combat forces." While this operational protection encompasses all warfare areas, there are few operations that pose the unique challenges of sea-based air defense—perhaps chief among them being the need for rapid response. Given the speed at which air defense operations take place, this arena potentially has more to benefit from dynamic bandwidth allocation than most. For this reason, an air detect-to-engage (DTE) scenario was chosen to demonstrate the effectiveness of Capabilities-based prioritization.

An air DTE scenario is the summation of air defense operations. It is divided into separate phases as the air defense team works to detect potential threats, classify them as such, identify the type of threat, and ultimately—if needed—engage those threats. While every DTE sequence may not culminate in an engagement, carrying the scenario through to its logical conclusion allows for observation of the full array of strike group operations in an air threat environment. As a result, the submarine and logistic support ships, which are usually part of a CSG composition, were set aside when developing the initial architecture description, as they do not provide any air defense capability.

Having established the scope of our research, we must now seek to understand the relationships between those operating within the CSG to conduct air defense. The following section seeks to capture those operational relationships and define the strike group architecture.

B. COMPOSITE WARFARE CONCEPT

1. Description of the Composite Warfare Concept

Generally, a command organization should be adaptive, yet straightforward in its execution (Vego, 2007). In order to be effective, information needs to be moved quickly from the gathering source to those who require it within the command organization. According to Vego, the fundamental prerequisites to a successful command and control (C2) architecture are: centralized direction and decentralized execution. These principles serve to reinforce the adaptive nature of the command organization while increasing the speed at which information can flow within its construct.

Vego states that the centralized direction principle establishes unity of command. While this somewhat inhibits lower level decision-making, this ideally supports the overall ability of the command organization to perform. Additionally, this principle provides the direction needed for the centralization of information-gathering and decision-making, thereby increasing the tempo of information movement (Vego, 2007).

The decentralized execution principle helps to counterbalance the limits placed on lower level commanders inherent to centralized direction. Ideally, the high level commanders specify only the objectives that need be accomplished (Vego, 2007). Authority is then delegated to the appropriate level to accomplish the objective, given that the objective is met following the established directives of the overall commander in charge. This concept allows for the maximum amount of flexibility within a command organization while not countermanding the principle of centralized direction.

Combined together, the concepts of centralized direction and decentralized execution form the backbone of the Composite Warfare Concept (CWC) (Morua, 2000). This concept of operation places the overall Carrier Strike Group Commander at the center of the information gathering hub. The Carrier Strike Group Commander is usually designated with the call sign BB (Bravo Bravo). His authority is then delegated to his subordinate commanders who exercise control over the warfare areas which they have been assigned (Morua, 2000). This organizational construct allows for the application of the two previously described fundamental principles: centralized direction and decentralized execution.

2. Application to the Carrier Strike Group

Under the CWC, BB assigns duties to each of his subordinate commanders (Morua, 2000). In terms of air defense, the relevant individual is the Air Warfare Commander—typically the commanding officer of the cruiser, designated BW (Bravo Whiskey). As such, he is responsible for the defense of the air space around the CSG.

Working with BW are the individual air defense units (ADUs), including the destroyers and the cruiser itself, acting as an entity separate from BW. Each of these air defense units contains an air defense team comprised of the following individuals:

- Commanding Officer (CO)—the CO has overall command of the individual ADU and is the only individual who may authorize release of offensive weapons. In this capacity, he represents the ship itself within the overarching air defense framework. He, meaning his ship, may be assigned tasking by BB in order to assist in the protection of the CSG but for the most part, operations are conducted according to a set of preplanned responses subject to negation by BB.
- Tactical Action Officer (TAO)—the TAO acts as the CO's representative in his absence and is delegated weapons' release authority for defensive purposes only. Though his responsibility extends to all warfare areas, the TAO is an integral member of the air defense team and all other air defense team members on his platform are subordinate to his direction. Communications to BB are typically conducted by the TAO for the CO, but operational control still flows through the CO.
- Combat Systems Coordinator (CSC)—the CSC is responsible for the coordination and management of all combat systems onboard. His position is unique in that he must be able to marry the concerns of both the tactician and the technician. Balance must be struck between mission priority and necessary repair. He is not a direct member of the air defense team, but his role as chief technician prevents his exclusion from this list. Additionally he is capable, at the CO or TAO's direction, of releasing the ship's weapons against a target. He is subordinate to the TAO.

- Anti-Air Warfare Coordinator (AAWC)—the AAWC is responsible for the coordination and de-confliction of the air space in and around the individual air defense unit. He works in conjunction with other AAWCs onboard the other air defense units and BW in order to identify and prioritize threats to the CSG. Additionally, he may receive tasking and direction by BB, via BW, for assets being controlled by his air defense unit or his unit itself. Most other members of the air defense team are subordinate to his direction, but he remains subordinate to the TAO. Like the CSC, the AAWC is capable, at the CO or TAO's direction, of releasing the ship's weapons against a target.

- Tactical Information Coordinator (TIC)—the TIC is responsible for maintaining the various Tactical Data Links (TADL) on which the ship is communicating. These links work to pass known track information from ship to ship, whether or not that ship actually holds that track with its own sensors. Working in conjunction with the TICs from the other air defense units and the strike group's Force Over the Horizon Track Coordinator (FOTC), the TIC de-conflicts link tracks and pushes identifications made by the air defense unit to the other ships in the strike group. He is subordinate to the AAWC.

- Missile System Supervisor (MSS)—the MSS is responsible for coordinating and relaying the status of the air defense unit's missile systems to the rest of the air defense team. Additionally, he must electronically release missiles being fired from his ship. He is primarily subordinate to the CSC for technical matters but coordinates with the AAWC and is subject to his direction.

- Radar System Coordinator (RSC)—the RSC acts in a similar fashion to the MSS, in that he is responsible for coordinating and relaying the status of the air defense unit's radar systems to the rest of the air defense team. Additionally, he is able to view raw radar data and can provide clarification for any ambiguous tracks the ship's radar holds. He is primarily subordinate to the CSC for technical matters but coordinates with the AAWC and is subject to his direction.

- Air Intercept Controller (AIC)—the AIC is responsible for coordinating and relaying the status of and direction to any tactical airborne fixed wing aircraft under the air defense unit's control. These aircraft are known as Defensive Counter Air (DCA) and may be used to identify potential hostile targets, escort targets of interest through the CSG's airspace, or actively engage hostile targets. While normally part of a carrier air wing, DCA become an extension of the ship controlling them while operating. The AIC is subordinate to the AAWC.

- Electronic Warfare Coordinator (EWC)—the EWC relays electronic sensor information from the ship's sensors and intelligence information from off ship sources. Working in conjunction with the strike group's Command & Control Warfare (C2W) Commander (BQ), the EW works to provide electronic warfare capability and intelligence information. He is subordinate to the AAWC.

Each of these individuals serves as an operational node within the architectural description of a carrier strike group. Their relationships may be captured through standard Department of Defense Architectural Framework (DoDAF) products and the structure of the strike group's architecture may begin to take shape.

3. Architectural Description

Based on the identified operational nodes, the roles, and their relationships to one another, an architectural description may be developed. The DoD guidance on *Architectural Framework Version 1.5, volume I*, identifies several important uses of architectures. One of these is for the description of mission areas. The use of an architectural description allows for the management of capabilities and the development of the enterprise architecture necessary to support that mission area. As such, DoDAF Version 1.5 may be used to capture the relationships between the operational nodes and guide the description of the mission area.

An Organizational Relationships Chart (OV-4) is useful for the clarification of the roles and responsibilities of each operational node (Figure 1). This diagram captures the overall command structure of the CSG and provides a simplified picture of the relationships between each operational node (DoD, 2007).

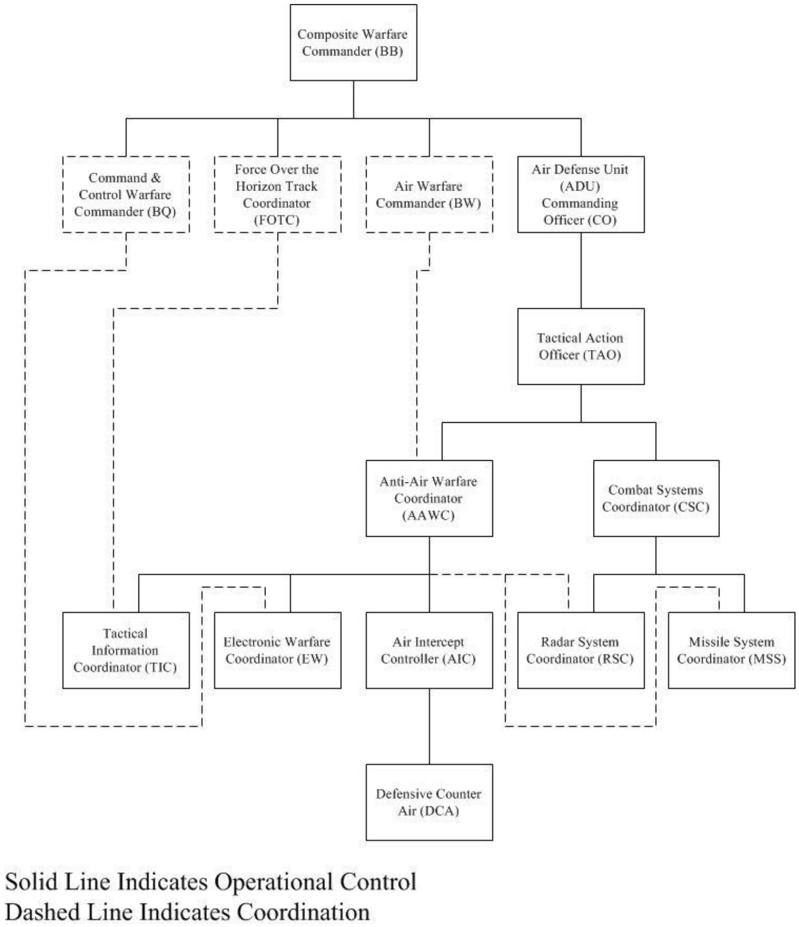
Composite Warfare Commander (BB)
Command & Control Warfare Commander (BQ)
Force Over the Horizon Track Coordinator (FOTC)
Air Warfare Commander (BW)
Air Defense Unit (ADU) Commanding Officer (CO)
Tactical Action Officer (TAO)
Anti-Air Warfare Coordinator (AAWC)
Combat Systems Coordinator (CSC)
Tactical Information Coordinator (TIC)
Electronic Warfare Coordinator (EW)
Air Intercept Controller (AIC)
Radar System Coordinator (RSC)
Missile System Coordinator (MSS)
Defensive Counter Air (DCA)
Solid Line Indicates Operational Control
Dashed Line Indicates Coordination

Figure 1. Strike Group OV-4, Organizational Relationships Chart

Given the defined parameters, an Operational Node Connectivity (OV-2) diagram can be developed to capture the structure of the strike group (Figure 2). According to the DoD guidance on Architectural Framework, this diagram serves to show the operational nodes and the communication needs between them. The communication (or need) lines show the flow of information between the operational activities. Each operational node has associated tasks which, when completed, aggregate to complete the overarching task of executing air defense operations.

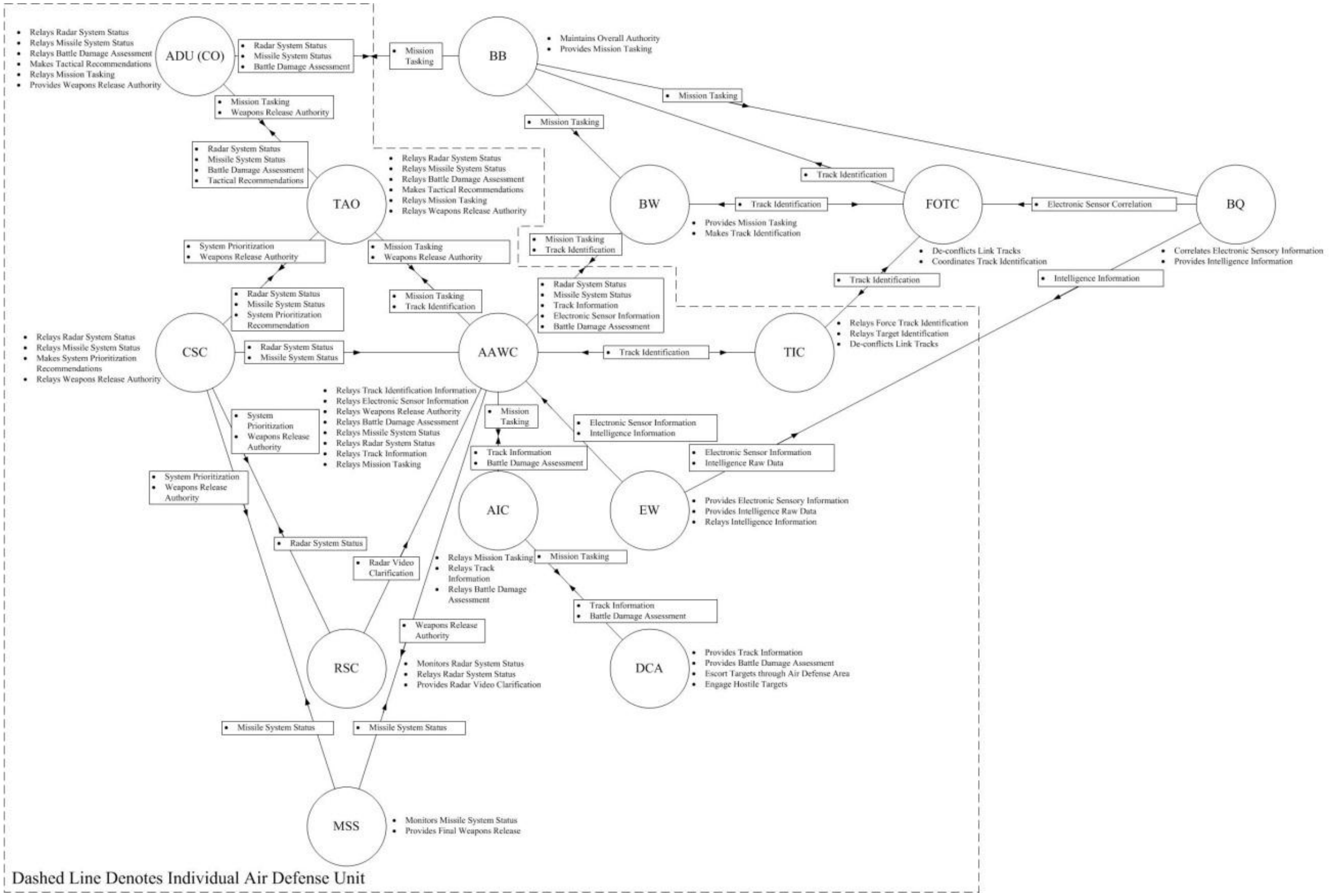
• Relays Radar System Status
• Relays Missile System Status
• Relays Battle Damage Assessment
• Makes Tactical Recommendations
• Relays Mission Tasking
• Provides Weapons Release Authority
ADU (CO)
• Radar System Status
• Missile System Status
• Battle Damage Assessment
• Mission Tasking
BB
• Maintains Overall Authority
• Provides Mission Tasking
• Mission Tasking
• Mission Tasking
• Weapons Release Authority
• Mission Tasking
• Radar System Status
• Missile System Status
• Battle Damage Assessment
• Tactical Recommendations
TAO
• Relays Radar System Status
• Relays Missile System Status
• Relays Battle Damage Assessment
• Makes Tactical Recommendations
• Relays Mission Tasking
• Relays Weapons Release Authority
• Track Identification
BW
• Track Identification
FOTC
• Electronic Sensor Correlation
BQ
• Provides Mission Tasking
• Makes Track Identification
• System Prioritization
• Weapons Release Authority
• Mission Tasking
• Weapons Release Authority
• Mission Tasking
• Track Identification
• De-conflicts Link Tracks
• Coordinates Track Identification
• Correlates Electronic Sensory Information
• Provides Intelligence Information
• Track Identification
• Intelligence Information
• Radar System Status
• Missile System Status
• System Prioritization Recommendation
• Mission Tasking
• Track Identification
• Radar System Status
• Missile System Status
• Track Information
• Electronic Sensor Information
• Battle Damage Assessment
• Relays Force Track Identification
• Relays Target Identification
• De-conflicts Link Tracks
• Relays Radar System Status
• Relays Missile System Status
• Makes System Prioritization Recommendations
• Relays Weapons Release Authority
CSC
• Radar System Status
• Missile System Status
AAWC
• Track Identification
TIC
• Relays Track Identification Information
• Relays Electronic Sensor Information
• Relays Weapons Release Authority
• Relays Battle Damage Assessment
• Relays Missile System Status
• Relays Radar System Status
• Relays Track Information
• Relays Mission Tasking
• System Prioritization
• Weapons Release Authority
• Mission Tasking
• Electronic Sensor Information
• Intelligence Information
• Track Information
• Battle Damage Assessment
• Electronic Sensor Information
• Intelligence Raw Data
• System Prioritization
• Weapons Release Authority
AIC
EW
• Provides Electronic Sensory Information
• Provides Intelligence Raw Data
• Relays Intelligence Information
• Radar System Status
• Radar Video Clarification
• Relays Mission Tasking
• Relays Track Information
• Relays Battle Damage Assessment
• Mission Tasking
• Track Information
• Battle Damage Assessment
• Weapons Release Authority
RSC
• Monitors Radar System Status
• Relays Radar System Status
• Provides Radar Video Clarification
DCA
• Provides Track Information
• Provides Battle Damage Assessment
• Escort Targets through Air Defense Area
• Engage Hostile Targets
• Missile System Status
• Missile System Status
MSS
• Monitors Missile System Status
• Provides Final Weapons Release
Dashed Line Denotes Individual Air Defense Unit

Figure 2. Air Defense OV-2, Operational Node Connectivity Diagram

Figure 2 illustrates the relationships between a single ADU and the off-ship warfare commanders and coordinators. The relationships pictured are duplicated for each ADU operating in the CSG. Coordination by the individual units independent of the Strike Group commander is rare and there is no command and control (C2) independent of the chain of command.

Using this architectural description, the systems required by each of the operational nodes to complete their assigned tasks can then be linked to the overall architecture description. This allows for the identification of those systems which are relevant to the overarching task of the air DTE and those which are not. In so doing, we can identify a prioritization scheme for information requiring transmission based on that information's relevance to the mission at hand. Our recommendation for the development of this process scheme will be presented in Chapter IV, but first we must understand the driving force behind this networked concept. The next section seeks to define the reason for this networked system approach and why such a prioritization scheme is necessary.

C. NETWORK-CENTRIC WARFARE

The Office of Force Transformation uses the term Network-Centric Warfare (NCW) to define the military operations and organizational structures that are emerging as forces become more networked together. This represents a paradigm shift from the idea of platform-centric operations to the encompassing of the "network" as a whole. Traditionally, platform-centric operations treated individual units as self-contained operators within their environment. In a network-centric environment, each platform comes equipped with services that can be "networked" together to achieve mission success. Is this context, network means not only the systems involved but also the operators behind those systems (Office of Force Transformation, 2005). As such, it is important to incorporate this understanding of the military organizational structure of the CSG as a network of systems and people into the way in which the organization operates—namely the Composite Warfare Concept (CWC), described in Section B of this chapter.

The PEO C4I Masterplan states that the purpose of NCW is to “increase combat effectiveness” through “information sharing” and providing “combined situational awareness” that acts to “accelerate C2 through synchronizing battle space efforts.” In order to combat the “fog of war,” battlefield commanders must be provided information that is time critical, accurate, and sufficient to increase situational awareness (SA). In this way, NCW serves to enable the CWC and increase the speed of command—getting sufficient, quality information to the decision maker as rapidly as possible and disseminating command decisions just as quickly (PEO C4I, 2010).

The Navy continues to take strides toward NCW, seeking to increase the robustness of information passed along the network and decrease the time for this information to get through. This movement toward NCW, epitomized by the Global Information Grid (GIG) concept, is curtailed by one thing—limited bandwidth (PEO C4I, 2010). As the volume of information demanded by end users increases, the constraints of the limited pipeline to push that information through become more evident. Bandwidth at sea is further limited by satellite availability and time sharing constraints, making for an even more challenging environment.

These challenges become clearer when applied to a tactical situation. Current surface warfare doctrine divides surface combat into three separate domains: air and missile defense, undersea warfare, and anti-surface warfare (Naval Transformation Roadmap, 2003). Each domain dictates its own requirements in terms of tactics and priorities. Often, surface combatants are faced with multiple, simultaneous threats operating within separate domains. As a result, non-collaborating shipboard systems may compete for limited bandwidth in order to push information to separate off-ship decision makers. This competition becomes even more intense as the threat level increases and the environment becomes more saturated with enemy combatants.

A distinction should be drawn between the idea of increasing the information flow to the decision maker and the idea of autonomy by lower-level decision makers. While bandwidth optimization can significantly increase the amount of information sent to the decision maker, it does nothing to affect the C2 organization in which it is being used. The DoD Office of Force Transformation identifies nine governing principles of NCW, among which is the idea of force *Self-Synchronization.* Self-Synchronization seeks to optimize the autonomy of subordinate forces to the point of self-re-tasking. This is accomplished through increased information dissemination and shared battle space awareness coupled with an understanding of "commander's intent" (Office of Force Transformation, 2005). Methodologies that increase the information flow rate but do not address the latency inherent to the traditional C2 organization—that is to say the speed of the networked response—are ultimately limited by the speed of command decision. This can be thought of as Industrial Age thinking that is being enabled by Information Age doctrine. As technology increases and NCW becomes the norm, it may be necessary to adjust the traditional command structure to fully capture the capabilities of the networked force.

The following chapter will define the Capabilities-based Competency Assessment approach we used to develop our proposed prioritization scheme. It will encompass the architectural descriptions we have defined here to establish justification for giving priority for one networked application over another. Next, a CSG operating environment and air DTE scenario will be developed which will stress current network capabilities. Using the developed scenario, we will evaluate both the current and our method for prioritizing bandwidth and the results of each will be compared and analyzed.

III. CAPABILITIES-BASED COMPETENCY ASSESSMENT

A. THE NEED FOR DYNAMIC BANDWIDTH ALLOCATION

While the Carrier Strike Group (CSG) serves a primarily national defense role, its use as a tool for U.S. foreign policy is both varied and vast. The President's 2010 National Security Strategy addresses the need for the U.S. to remain the world leader in responding to natural disasters. Natural disasters continue to pose a serious risk to civilians worldwide. Given the large amount of resources at its disposal, the ability to reach distant locations in a timely manner, and its inherent flexibility, the CSG often acts as the first American response to natural disasters both in the U.S. and abroad. Recent examples include the *USS CARL VINSON (*CVN 70*)* response to the 2010 earthquake in Haiti, the *USS RONALD REAGAN (*CVN 76*)* 2011 response to the earthquake and subsequent tsunami in Japan, and the 2004 *USS ABRAHAM LINCOLN (*CVN 72*)* response to the tsunami in the Indian Ocean.

System priorities and demands vary greatly from traditional CSG roles to that of disaster relief. While air defense operations are imperative to the defense of the carrier, they do little to assist in a disaster relief scenario. Air operations move from providing defense capability to enabling the movement of supplies and evacuation of the wounded. Strike groups' command and control architecture must be able to encompass not only U.S. military agencies but also international military and non-government organizations as well, moving from the classified to the almost entirely unclassified domain. Given the inherent flexibility of the CSG, it provides a common sense response to international tragedy; but in order to fully maximize the capabilities of the CSG, network priorities must be able to shift. While it is important that the defensive capabilities of the CSG remain in place, they may find themselves in a reduced role during times of disaster relief.

This idea extends logically to varying tactical missions as well. The priorities during air defense operations are not necessarily the same as those during an anti-submarine scenario or even normal underway steaming. The heavy intelligence gathering requirements of a strike or air defense mission do not reflect the intensive processing inherent to defeating an enemy submarine. Likewise, the administrative burden of normal underway steaming can take priority during times of peace but should fall by the wayside in a wartime environment—given such a burden would detract from the mission of defending the ship. If priority is not given to mission critical applications as they relate to the mission at hand, network capability is not optimized and as a result, the overall effectiveness of the CSG is diminished.

The idea of mission-based network prioritization has not been lost on the fleet at large. There is an increased demand for the ability to modify Quality of Service (QoS) priorities, based on mission specific tasking (Rambo, 2011). The benefit of this approach is that it can reduce network response times and increase network throughput according to what the mission commander needs. When information gets to the decision maker faster, there is more time to develop the "right" decision. By developing the ability to provide dynamic bandwidth allocation at the application level, shipboard services may be prioritized correctly and more quickly based on the mission priorities—thus leading to increased mission effectiveness and less wasted network resources.

B. CURRENT BANDWIDTH ALLOCATION SCHEME

The Navy's system for the allocation of bandwidth at sea is the Automated Digital Network System (ADNS). Initially fielded in the late 1990s, ADNS works by routing data that is outbound from the ship through the various Radio Frequency (RF) paths available for its transmission (Rambo, 2011). One of the important capabilities of ADNS is the delivery of basic Quality of Service (QoS) capability. QoS enables the network to make "smart" decisions when available network resources are overtaxed by the amount of information they are being required to route (Rambo, 2011). Without QoS, all shipboard network traffic would compete for the same RF pipeline and there is no ability to prioritize information.

Subsequent variants of ADNS have allowed for improved bandwidth management and enhanced QoS administration; however, there is still room to improve the QoS capability. The current ADNS variant, Increment Three (ADNS INC III), enables QoS through static application prioritization. ADNS works to mark data packets generated by these applications and then transmits them through a “packetshaper” which assigns a priority to the traffic being transmitted. These packets are then sorted into bins according to their assigned prioritization and transmitted accordingly. This prioritization scheme is set by the Naval Cyber Forces (NCF) command and can only be modified through an extended process and is not subject to change by ship’s force (Rambo, 2011).

Shipboard networks are divided into Top Secret/Sensitive Compartmentalized Information (TS/SCI), Secret, Unclassified, and a separate Coalition classification enclaves. There is an additional enclave dedicated to network overhead and encryption. Data packets generated by shipboard applications are marked using the Type of Service IPv4 header at a packet shaper operating with each classification enclave and routed to various network queues based on this marking operating within ADNS (Automated Digital Network System, 2011). Each queue is guaranteed a minimum amount of bandwidth allocated to it. Once these data packets have been routed to their appropriate queues, transmission is dictated by either First In First Out (FIFO)—i.e., the first data packet to arrive is the first to leave—or by Cisco Weighted Random Early Detection (WRED). WRED works by having the network router (ADNS is this case) randomly drop IP packets being sent by applications. This dropping of packets causes the application transmitting those packets to assume network congestion and slow down the rate of transmission. The packets are dropped based on a given probability schedule. Applications given a higher priority are assigned a lower probability of drop and thus, a higher throughput. This weighting is done via a formal submission process and the application priority is validated by Naval Cyber Forces (Rambo, 2011). Additionally, if applications are not utilizing the minimum bandwidth allowance, that bandwidth is shared with other applications.

Given the changing priorities of separate mission areas, it is imperative that shipboard personnel be able to assign prioritizations dynamically to shipboard network services. This need continues to grow as the Navy’s Consolidated Afloat Networks and Enterprise Services (CANES) system is fielded.

Per SPAWAR's CANES website, CANES will serve to consolidate and replace five existing legacy networks afloat. These systems include Integrated Shipboard Network System (ISNS), Sensitive Compartmented Information (SCI) Networks, and Combined Enterprise Regional Information Exchange System Maritime (CENTRIXS-M). Through the utilization of the Service-Oriented Architecture (SOA) concept, CANES will eliminate redundant legacy hardware and replace them with a single, consolidated system. According to the CNO's CANES Initial Implementation and Action Message, DTG 071927Z DEC 09, all shipboard systems that will be fielded after the implementation of CANES must be compatible with the new common network hardware. This single, common computing environment provides the necessary framework to implement Quality of Service (QoS) at this level of granularity. Since all applications will be housed on a single network, control will encompass every possible system regardless of mission.

C. THE CAPABILITIES-BASED COMPETENCY APPROACH

Recent efforts by the Naval War College have developed an approach to manpower analysis known as Capabilities-based Competency Assessment (CBCA). CBCA differs from traditional manpower analysis in that it seeks to identify functional roles working within a team construct versus looking at billets and shipboard occupations (Suttie & Potter, 2008). These functional roles are linked to identified "subtasks" which aggregate to complete mission level tasking. The major distinction of CBCA is the focus on capability versus a set of competencies (Suttie & Potter, 2008). Suttie and Potter provide the example of a plumber. CBCA is not concerned with making a better plumber by understanding what he does; instead CBCA seeks to understand the role of the plumber in the upkeep of a home. It is not important for the homeowner to understand how the plumber fixes his sink, only his relationship to the plumber and the capability that he provides. Once the *capability* inherent to the role is understood, its relationship to other roles working in the total system can be comprehended.

The end goal of CBCA is to solve the disparity between the needs of the Operational Commander to complete mission specific tasking and the legacy manpower and system requirements which are inherent to the more traditional manpower approaches. This is accomplished by linking mission essential task lists (METLs) to the personnel and systems required to complete them. Such an approach departs from the traditional, billet-based, allocation of personnel and seeks to define “roles” which act as critical nodes that correspond to a Department of Defense Architectural Framework (DoDAF) Operational Node Connectivity Description (OV-2) (Suttie R. D., 2011) of the overall operational architecture. These roles would act independently of the personnel assigned to complete them; however, training pipelines would ideally be tailored to fill those roles.

This study applies the process of Capability-Based Competency Assessment (CBCA) to identify METLs which can then be used to identify a set of competencies which incorporate operations, personnel, and system requirements inherent to air defense operations as suggested by Suttie & Potter (2008). These competencies act as operational nodes on which the high level architecture is developed. Defining such an architecture is a crucial first step in understanding the impact of Service-Oriented Architecture and capturing the benefits of its deployment. The end goal of this high level architecture is to improve command and control and aid the decision maker at the enterprise level. Operating at this level of abstraction, it is imperative that the architecture capture not only the people or processes to be implemented, but also the links between the processes and the methods for completing those processes.

The Service-Oriented Architecture framework is formed by assigning METLs to the operational nodes responsible for their execution and which are completing activities which aggregate to complete an overarching high-level activity. These relationships are captured by an Operational Activity Model Description (OV-5). This model may be completed in conjunction with a Systems Functionality Description (SV-4), which not only captures the decomposition of the top-level activity, but also identifies the systems used to enable functionality. Finally, the relationships between the operators, their responsible actions, and the systems used to complete those actions are captured via an Operational Activity to Systems Function Traceability Matrix (SV-5a). By doing so, the relationships between the operational nodes and the systems that each node uses to accomplish those tasks are identified.

This approach ensures that the operational nodes and services are aligned within the overall system architecture and commanders are able to more effectively leverage existing network resources to accomplish required tasks within a compressed time frame based on identified mission priorities. These products are used to understand the relationships between operator and machine and allow the warfare commander to assign the correct prioritization to the systems at his disposal. Once form has been matched to function, it is possible to understand which nodes and, as a result, which systems are needed to complete an aggregate task. This process provides justification and realization of the most beneficial arrangement for network prioritization. By assigning the highest level of prioritization to those network applications needed to accomplish mission appropriate tasking, a strike group's network resources are used to their fullest capability. The performance of all other systems which are not crucial to the completion of the assigned tasking should be sacrificed in order to benefit those that are imperative.

D. DEFINING THE OPERATIONAL NODES

Before system prioritization can take place, it is essential to identify the users that will operate those systems. For the purpose of our study, these users have already been identified. The operational nodes from the Operational Node Connectivity (OV-2) diagram defined in Chapter II will be used for our CBCA analysis. The second step is to identify the tasks associated with each user for the purpose of completing air defense operations. These tasks too have already been identified and analyzed. They are listed within the Navy's Universal Naval Task List discussed in the next paragraph.

The Universal Naval Task List (UNTL) serves as a repository for tasks that can be completed by Naval forces. Defined as the what, not necessarily the how, of Naval warfare, the UNTL is used by commanders to determine what can be done by the Naval elements under their command. Mission essential task lists (METLs) are derived from this list and are used to support a commander's assigned mission. They serve as a command's list of tasks that are considered essential for mission accomplishment (Chief of Naval Operations, Commandant, United States Marine Corp, Commandant, United States Coast Guard, 2007). For example, if a commander wanted the ships under his command to move, he would consult the Navy Tactical Tasks (NTA) 1.1 Move Naval

Tactical Forces. Under this task are the subtasks associated with ship movement. The subtasks that the commander deems to be important would be identified and the units under his command must prepare to be able to meet those tasks as defined in the documentation associated with them.

By parsing this list of mission capabilities and identifying those relevant mission tasks, it becomes possible to prioritize tasks based on their relevance to the mission at hand. The next logical step is to assign the information systems required to accomplish those tasks the same level of priority to develop the final scheme for appropriate bandwidth allocation.

E. SUBTASKS REQUIRED FOR AIR DEFENSE OPERATIONS

We can now examine the UNTL. The UNTL is subdivided into separate task levels for each level of warfare. The prefix for tactical level tasks is TA, thus Naval tasks at the tactical level are known as Navy Tactical Tasks (NTA). An examination of the UNTL reveals which NTA's are relevant to air defense is provided in Table 1. By using the descriptions provided in the UNTL for each NTA, it is possible to compile a succinct list of those tasks which are related to air defense and which can then be analyzed.

	Task	Task Name
NTA 2 Develop Intelligence	NTA 2.1	Plan and Direct Intelligence Operations
	NTA 2.2	Perform Collection Operations and Management
	NTA 2.2.1	Collect Target Information
	NTA 2.2.3	Perform Tactical Reconnaissance and Surveillance
	NTA 2.3	Process and Exploit Collected Information and Intelligence
	NTA 2.4	Conduct Analysis and Produce Intelligence
	NTA 2.5	Disseminate and Integrate Intelligence
	NTA 2.6	Evaluate Intelligence Operations
NTA 3 Employ Firepower	NTA 3.1	Process Targets
	NTA 3.1.5	Conduct Tactical Combat Assessment
	NTA 3.2	Attack Targets
	NTA 3.2.5	Conduct Electronic Attack
	NTA 3.2.7	Intercept, Engage, and Neutralize Enemy Aircraft and Missile Targets
NTA 5 Exercise Command and	NTA 5.1	Acquire, Process, Communicate Information, and Maintain Status
	NTA 5.2	Analyze and Assess Situation
	NTA 5.4	Direct, Lead, and Coordinate Forces
	NTA 5.5	Conduct Information Warfare (IW)
	NTA 5.5.4	Conduct Electronic Warfare Support (ES)
NTA 6 Protect the Force	NTA 6.1	Enhance Survivability
	NTA 6.1.1	Protect Against Combat Area Hazards
	NTA	Positively Identify Friendly Forces
	NTA 6.5	Perform Consequence Management
	NTA 6.5.2	Coordinate Damage Control Operations

Table 1. Air Defense NTAs (After Universal Naval Task List, by Chief of Naval Operations, Commandant, United States Marine Corp, Commandant, United States Coast Guard, 2007, Washington, DC: Chief of Naval Operations; Commandant of the Marine Corps; and Headquarters United States Coast Guard).

The DoD guidance on *Architectural Framework Version 1.5, volume II*, defines an OV-5, Operational Activity Model, as describing the operations conducted to complete a mission. It provides the flow between operational activities and when used with an OV-2, Operational Node Connectivity Diagram, it serves to identify the operational nodes responsible for those activities.

An OV-5 (Figure 3) is constructed by taking each of the NTA's identified as relevant to air defense operations as presented in Table 1, establishing a hierarchy of those tasks, and mapping each NTA to the operational node responsible for its completion. This description may later be used to assist in mapping the systems used by the operational nodes to complete their assigned tasking.

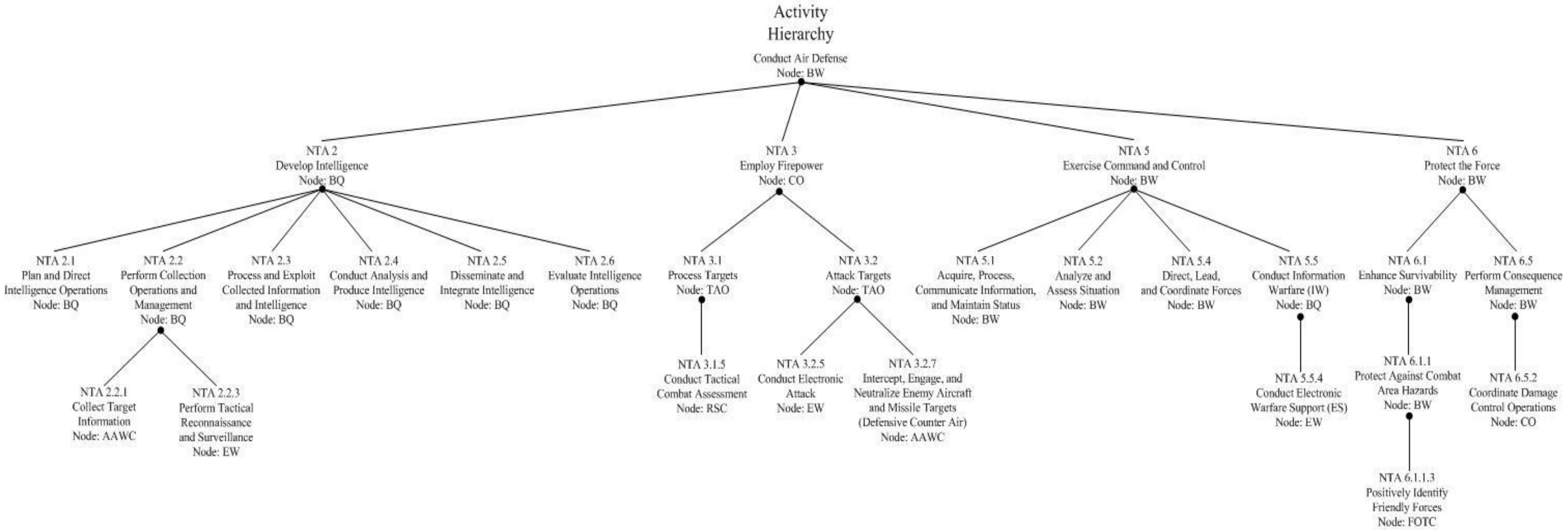

Figure 3. Conduct Air Defense OV-5, Operational Activity Model

Several of the mid-level functions appear to be decomposed by only one sub-function. For example, NTA 3.1 Process Targets is decomposed only by NTA 3.1.5 Conduct Tactical Combat Assessment. This is due to the arrangement of the UNTL. NTA 3.1 is actually decomposed by several sub NTAs, but not all of them are applicable to air defense. In order to simplify the diagram, only those sub-functions which were relevant to air defense operations were recorded in Figure 4.

Having identified the operational activities involved in the process of conducting air defense and linking the each of these activities to the operational node responsible for their completion, the next step in our process to tie in the systems that each of those operational nodes require to complete their assigned tasking. Linking this form to function will provide the justification for our prioritization scheme. The next section is dedicated to identifying those systems and mapping their relationship to each other.

F. IDENTIFYING REQUIRED SYSTEMS FOR AIR DEFENSE OPERATIONS

The Command, Control, Communications, Computers, and Intelligence (C4I) Masterplan serves to summarize the major attributes of DoN network-centric systems. The Masterplan categorizes ships types at different levels. Aircraft carriers are identified as Force Level Ships, Cruisers and Destroyers Group Level. It provides C4I system baselines for each of these ship types as projected through FY12. These baseline descriptions may be used to determine those systems which communicate via ADNS and could therefore, benefit from network prioritization. By using the system descriptions presented in the C4I Masterplan, a list was developed of those systems required to conduct air defense operations (Table 2).

System Name	Description	Ship Type
Ship's Signal Exploitation Equipment (SSEE) Increment E/F	Provides: 1) Direction finding (DF) 2) Signal acquisition 3) Hostile Forces Integrated Targeting Service (HITS), 4) Digital Receiver Technology (DRT) geolocation capability 5) Integrated signal analysis and select National Security Agency (NSA) applications via the Cryptologic Unified Build (CUB) toolbox	CVN, CG, DDG
AN/USQ-172(V)10 Global Command and Control System – Maritime (GCCS-M)	Provides: 1) Unit location and amplifying information 2) Fuses, correlates, filters, maintains and displays location and attribute information on friendly, hostile and neutral land, sea and air forces, integrated with available intelligence and environmental information to develop Common Operational Picture (COP) 3) Aides decision maker	CVN, CG, DDG
Distributed Common Ground System – Navy (DCGS-N)	Provides: 1) Integrates shared intelligence data, information and services between various intelligence and decision making entities 2) Distributable intelligence products	CVN
Naval Integrated Tactical Environment System, Variant IV (NITES-IV)	Provides: 1) Operational and tactical METOC support to Navy, Marine Corps and Joint Forces engaged in worldwide operations, ashore and afloat 2) Distributes gathered meteorological data	CVN

Table 2. Air Defense Net-Centric Systems (After PEO C4I 2011). PEO Master Plan Version 5.0. San Diego: Program Executive Officer, Command, Control, Communications, Computers and Intelligence.

It should be noted that while the systems chosen provide a good representative sample of those systems which may be used in air-defense operations, this list should by no means be considered exhaustive. The C4I Masterplan provides only system overviews and does not give detailed explanations of each system and its capabilities. In order to correctly identify each relevant system, subject matter experts on each would need to be consulted and personnel familiar with the entire C4I portfolio would need to compile an exhaustive list. For our purposes, however, it is sufficient to include these systems to validate our approach.

Using these systems, we may now seek to capture the capabilities each one provides. This may be accomplished using a System Functionality Description. The next section will outline the process for developing this DoDAF viewpoint and how it will be used.

G. SYSTEM FUNCTIONALITY DESCRIPTION

The DoD guidance *on Architectural Framework Version 1.5, volume II*, defines a SV-4a, System Functionality Description, as documenting system functional hierarchies and system functions and how data flows between them. This product is closely related to the OV-5 and, when used in conjunction with the SV-5a viewpoint, will provide a mapping to the operators and the systems they use.

A SV-4a (Figure 4) is constructed by taking each of the systems identified as relevant to air defense operations and breaking them down to their provided functionality. The relationships between those systems are then mapped, providing the structure of the viewpoint.

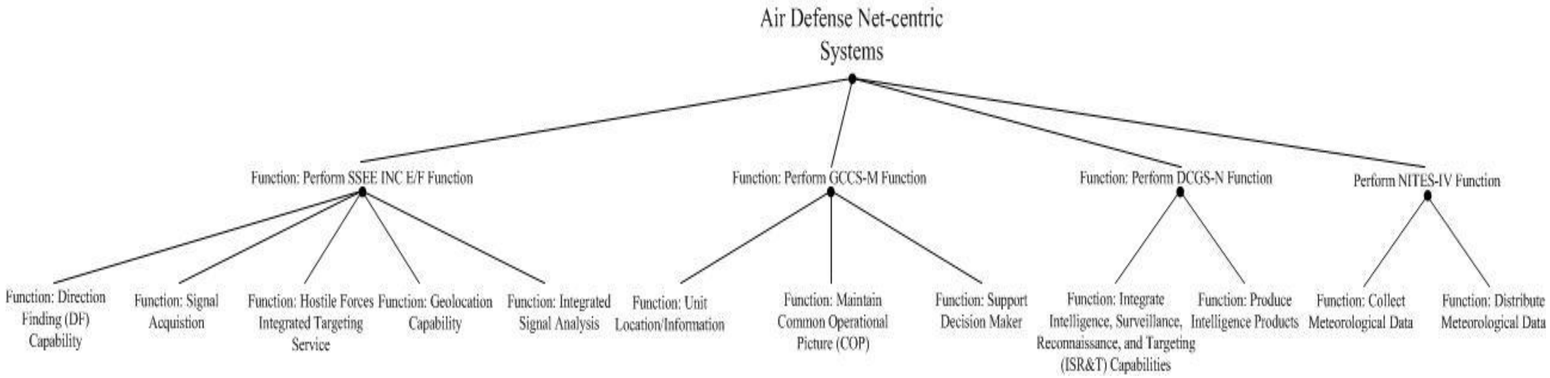
Air Defense Net-centric Systems
Function: Perform SSEE INC E/F Function
Function: Perform GCCS-M Function
Function: Perform DCGS-N Function
Perform NITES-IV Function
Function: Direction Finding (DF) Capability
Function: Signal Acquistion
Function: Hostile Forces Integrated Targeting Service
Function: Geolocation Capability
Function: Integrated Signal Analysis
Function: Unit Location/Information
Function: Maintain Common Operational Picture (COP)
Function: Support Decision Maker
Function: Integrate Intelligence, Surveillance, Reconnaissance, and Targeting (ISR&T) Capabilities
Function: Produce Intelligence Products
Function: Collect Meteorological Data
Function: Distribute Meteorological Data

Figure 4. Conduct Air Defense SV-4a, System Functionality Description

Having now identified the functionality each air-defense unit provides, we can link the system function to the operational tasks we previously identified. This is completed using an Operational Activities to Systems Functional Traceability Matrix and will be developed in the next section.

H. LINKING OPERATIONAL ACTIVITIES TO SYSTEMS FUNCTIONS TRACEABILITY MATRIX

The DoD guidance in *Architectural Framework Version 1.5, Volume II*, defines a SV-5a (Figure 5) as documenting the relationship between the operational activities and system functionality present in the overall architecture. It is this relationship that is most beneficial for the purpose of this thesis.

By identifying the systems being utilized by operators to complete assigned tasking, it is possible to document those systems which are most relevant to the overarching task at hand. Given their usefulness, these systems are the ones which should be given priority over other networked systems in a bandwidth constrained environment. Our methodology provides a logical justification for giving priority to one system over another and demonstrates a step-by-step process by which justification for the prioritization of networked systems may be derived. This methodology can be recreated depending on the mission at hand to develop the correct network prioritization based on mission needs.

OPERATIONAL ACTIVITIES		SYSTEM FUNCTIONS											
		SSEE INC E/F					GCCS-M			DCGS-N		NITES - IV	
		1) Direction Finding (DF) Capability	2) Signal Acquisition	3) Hostile Forces Integrated Targeting Service	4) Geolocation Capability	5) Integrated Signal Analysis	1) Unit Location/Information	2) Maintain Common Operational Picture	3) Support Decision Maker	1) Integrate Intelligence, Surveillance, Reconnaissance, and Targeting Capabilities	2) Produce Intelligence Products	1) Collect Meteorological Data	2) Distribute Meteorological Data
RSC	NTA 3.1.5 - Conduct Tactical Combat Assessment									╲	╲	╲	╲
EW	NTA 5.5.4 - Conduct Electronic Warfare Support (ES)	X	X	X	X	X				╲	╲	╲	╲
	NTA 3.2.5 - Conduct Electronic Attack									╲	╲	╲	╲
	NTA 2.2.3 - Perform Tactical Reconnaissance and Surveillance	X	X	X	X	X				╲	╲	╲	╲
AAWC	NTA 3.2.7 - Intercept, Engage, and Neutralize Enemy Aircraft and Missile Targets (Defensive Counter Air)									╲	╲	╲	╲
	NTA 2.2.1 - Collect Target Information									╲	╲	╲	╲
TAO	NTA 3.2 - Attack Targets									╲	╲	╲	╲
	NTA 3.1 - Process Targets						X	X	X	╲	╲	╲	╲
CO	NTA 6.5.2 - Coordinate Damage Control Operations									╲	╲	╲	╲
	NTA 3 - Employ Firepower									╲	╲	╲	╲
FOTC	NTA 6.1.1.3 - Positively Identify Friendly Forces						X	X	X				
BQ	NTA 5.5 - Conduct Information Warfare (IW)	X	X	X	X	X							
	NTA 2.6 - Evaluate Intelligence Operations									X	X		
	NTA 2.5 - Disseminate and Integrate Intelligence						X	X	X	X	X		
	NTA 2.4 - Conduct Analysis and Produce Intelligence						X	X	X	X	X	X	X
	NTA 2.3 - Process and Exploit Collected Information anc Intelligence									X	X		
	NTA 2.2 - Perform Collection Operations and Management	X	X	X	X	X				X	X		
	NTA 2.1 - Plan and Direct Intelligence Operations									X	X		
	NTA 2 - Develop Intelligence	X	X	X	X	X	X	X	X	X	X	X	X
BW	NTA 6.5 - Perform Consequence Management												
	NTA 6.1.1 - Protect Against Combat Area Hazards												
	NTA 6.1 - Enhance Survivability												
	NTA 6 - Protect the Force												
	NTA 5.4 - Direct, Lead, and Coordinate Forces						X	X	X				
	NTA 5.2 - Analyze and Assess Situation						X	X	X	X	X		
	NTA 5.1 - Acquire, Process, Communicate Information and Status	X	X	X	X	X				X	X	X	X
	NTA 5 - Exercise Command and Control						X	X	X				

Figure 5. Conduct Air Defense SV-5a, Systems Function Traceability Matrix

The X’s on the SV-5a indicate those systems which are being used by an operator to complete a task. For now, only those systems which connect to the Global Information Grid (GIG) via an Internet Protocol (IP) pipeline have been mapped. As new systems are fielded to be deployed on CANES, this diagram would need to grow to encompass them. The dashed area indicates that those systems identified that are not currently available for those users.

ADNS currently recognizes 54 separate application types (Automated Digital Network System, 2011). These applications are spread over four classification levels—Top Secret, Secret, Unclassified, and Coalition—and one network overhead classification. Each of these applications is mapped to one of 13 separate named queues. Using the Capabilities-based Competency Assessment (CBCA) developed in this chapter, we can map the applications ADNS recognizes to those systems identified as being important to our mission, air defense operations (Table 3).

System Name	**Application Types**
SSEE INC E/F	Time Sync, Chat, COP, HFDF
	E-mail, CERCIS, OS/BS, PARA 126, TDDS
	Name Resolution, Encryption, File Transfer, Web, Secure Web, Remote Access, Targeting PSAS
	EVCP, Big Brother, ISRT
GCCS-N	GCCS-M NETPREC, Critical E-mail/Web
DCGS-N	High Priority Applications
NITES-IV	

Table 3. Mapping System Names to Application Types

Each information system has now been linked to the task associated with its use and each task has been linked to the operator who completes that task. Our proposed prioritization scheme will place each of the identified systems at the top of the priority scheme. A detailed comparison of the current priority scheme and our proposal will be outlined in the Chapter VI, but first we will define an environment in which to test the effectiveness of our proposal.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. AIR DETECT-TO-ENGAGE SCENARIO

To vet the effectiveness of increased flexibility in bandwidth allocation, a typical air detect-to-engage (DTE) scenario will be developed. This scenario will be used to compare the time effects of the proposed bandwidth allocation scheme, based on operational tasks and warfighter information needs, to the static bandwidth allocation scheme inherent to ADNS INC III.

First, an operational environment must be chosen and defined for the scenario. Next, an initial force laydown for the Carrier Strike Group (CSG) will be established. Finally, a threat will be chosen and deployed against the CSG. The scenario will then progress through the incremental stages of the air DTE sequence, ultimately culminating in an engagement of the threat by friendly forces. This scenario will be simulated using both methods of bandwidth allocation and comparisons will be drawn in terms of time and effectiveness.

A. THE ENVIRONMENT

Throughout history, most naval combat has taken place close to the shore versus the open ocean (Vego, 2007). The reason for this is rooted in Mahan's theory of naval operations, namely the purpose of a nation's navy is the protection of its commercial interests. Commercial shipping is linked to a nation's ports, which lay on the nation's coast. This idea, coupled with the need for the Navy to be able to project power inland, has pushed the emphasis of Naval strategy toward the *littoral* – i.e., close to shore – environment. In 2007, the Navy, Marine Corp, and Coast Guard published the first ever joint strategic document entitled, *A Cooperative Strategy for 21st Century Seapower*. This document outlines the need to maintain the capability to project power ashore as well as support for forces once ashore. Integral to this strategy are operations within the littoral environment. For this reason, a representative littoral environment will act as the theater for the scenario.

A fictional littoral area of approximately 250 x 350 nautical miles in dimension will serve as the operating area for the carrier strike group (CSG). The environment consists of the fictional country Gray's coastline, including its capital, Capital City, and another large coastal city, Graytown (Figure 6).

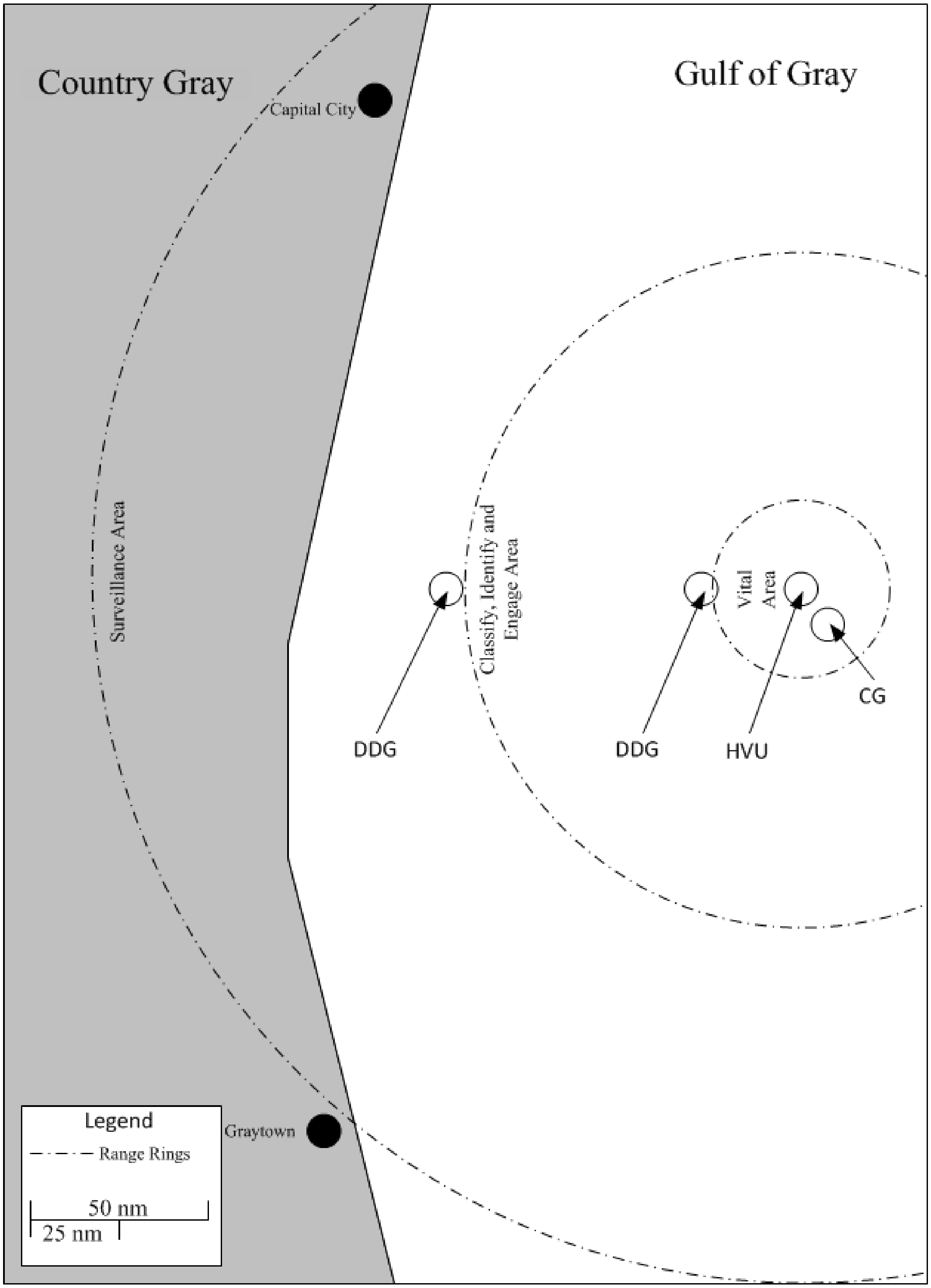

Figure 6. CSG Operating Environment

B. FORCE LAYDOWN

The CSG is deployed approximately 150 miles from the coastline of country Gray. This placement allows time for any potential threats to the CSG to progress through the various concentric air defense zones of the strike group – denoted by the Range Rings in Figure 3. These air defense zones are defined as follows:

- Vital Area (VA)—the VA is defined as the area which extends from the high-value unit (HVU) to the maximum range of enemy weapons which may be employed against the HVU. Based on the threat which will be evaluated, the VA is centered on the aircraft carrier and extends out to a radius of 20 nautical miles.
- Classify Identify and Engage Area (CIEA)—the CIEA is defined as the area which extends to the maximum range of friendly weapons that may be employed against hostile targets. It is so named because the goal of the air defense team is to classify and identify all potential threats in this area and, if warranted, engage hostile enemy units prior to their arrival in the VA. The primary surface-to-air weapon of the U.S. fleet is the Standard SM-2 MR, RIM-66C missile (Polmar, 2005). The SM-2 has a maximum range in the vicinity of 80 nautical miles and will serve as the delineator of the CIEA's range. While technically the CIEA morphs to accommodate the force laydown, with each air defense unit having a CIEA based on its own weapons range, this would unnecessarily complicate the battle problem. As long as consistency is maintained between the two simulations, the CIEA may be simplified and centered on the HVU.
- Surveillance Area (SA)—the SA is defined as the area which extends to the maximum detection range of the CSG's sensors. In this case, there are three AEGIS warships, equipped with the SPY-1 radar system, which has a detection range in the order of 200 nautical miles (Polmar, 2005). While identification and classification of potential targets operating in this area is not crucial, it is desirable to do so in preparation for their entry into the CIEA. Similar to the CIEA, the SA changes with the force laydown but will be modified to be centered on the HVU and extend out to a range of 200 nautical miles.

The notional force consists of one *Arleigh Burke Class* guided missile destroyer (DDG) positioned 100 nautical miles (nm) west of the HVU, a second *Arleigh Burke Class* DDG positioned 25 nm west of the HVU, and a *Ticonderoga Class* CG positioned 10 nm to the southeast of the HVU.

While typically multiple Defensive Combat Air (DCA) units would be deployed for the protection of the strike group, the purpose of this scenario is to evaluate the effectiveness of shipboard systems and operators based on a proposed bandwidth prioritization scheme. DCA would normally act as the primary means to engage potential threats against the CSG, but using them in this capacity may introduce unnecessary variations in the scenario results. For this reason, DCA deployment will not be considered in this scenario.

C. THE THREAT

The McDonnell Douglas F-4 Phantom was introduced to the U.S. military in 1958 and began to be sold internationally by 1964. Production continued form 1958 to 1979, with a total of 5,195 aircraft constructed. Although retired by the U.S. in 1996 there are still more than 800 F-4 Phantom IIs active in eight air forces worldwide and the aircraft will most likely remain in service until at least 2015 (F-4 Phantoms Phabulous 40th). The F-4 was designed to carry up to 16,000 lbs. of external armaments and provided multi-role capability including long range attack and is equipped with look-down/shoot-down capability (McDonell Douglas F-4D, 2009). Given its long history of service, wide dissemination, and capabilities as an attack aircraft, the F-4 Phantom will serve as the threat aircraft for this scenario.

According to the National Museum of the U.S. Air Force website, the basic characteristics of the F-4 are as follows:

Manufacturer: McDonnell Douglas

Armament: Up to 16,000 lbs. external conventional/nuclear bombs, rockets, missiles or 20mm cannon

Propulsion: Two General Electric J-79-GE-15s of 17,000 lbs. thrust, each with afterburner

Altitude: Up to 40,000 ft.

Speed: 1,178 knots at 35,000 ft.

Radius: 250 nm

The CHETA C-801/CSS-N-4 *SARDINE* is a Chinese developed anti-ship cruise missile believed to be developed from the French *EXOCET* (Pike, 2011). The C-801, and several of its derivatives, has been successfully launched from fighter aircraft, including the F-4. The missile has been successfully tested against and sunk a test target ship with a displacement of 10,000 tons. Equipped with a 165 kg high explosive, semi-armor piercing warhead, maximum effective range in excess of 40 km, and an anti-jamming terminal guidance system, the C-801 missile continues to be a viable threat to U.S. forces operating in littoral environments. For this reason, the C-801 will serve as the threat missile against the force.

The Naval Institute Guide to World Naval Weapons Systems provides the following characteristics for the C-801:

Manufacturer: CHETA—China Hai Yang [Sea Eagle] Electro-Mechanical Technology

Armament: 167 kg, semi-armor piercing warhead

Propulsion: Boost-sustain rocket (two motors)

Altitude: Cruise: 20–30 meters; Attack: 5—7 meters

Speed: 0.9 mach (595 knots)

Radius: Approximately 40 km

D. THE SCENARIO

The operational scenario will consist of three phases: *surveillance, escalation, engagement.* The purpose of each of these phases will be to simulate likely operating conditions and threat and warning conditions, and to determine the effectiveness of dynamic bandwidth allocation.

1. Surveillance Phase

During this phase, the ships in the operating environment will conduct normal operations inherent to underway steaming. This phase of the scenario will last thirty minutes to provide ample time for the network to reach steady-state operations and to provide a reasonable period of observation. In our model, it will be used to determine the time required for information to be transmitted off the different classes of ships to be relayed back to decision makers within the strike group. This will be accomplished using the settings inherent to ADNS INC III and the results will be used to gauge the effectiveness of the current settings. Upon conclusion of this phase, it will be assumed that the strike group commander will receive information of an impending attack on the CSG and will increase his air defense posture accordingly.

2. Escalation Phase

During this phase, the threat F-4 equipped with the C-801 missile will take off from Graytown and proceed northeast towards the HVU. It will climb to its cruising altitude and attempt to launch its weapon against the aircraft carrier at the earliest opportunity.

The purpose of this phase will be to compare the difference in transmission times under the proposed prioritization scheme and the legacy settings and evaluate the impact on the *human* decision making process. This will require an assessment of not only statistical significance between the data sets but also practical significance in terms of the speed of human thought.

During this phase, there will be an increase in network traffic associated with the identification of the F-4. Measurements of data latency and throughput will be recorded for each prioritization scheme, which will allow us to draw a contrast between the two. This phase will terminate once the F-4 has reached its earliest firing opportunity.

3. Engagement Phase

The final phase of this scenario will assume the F-4 has successfully transited the CIEA and deployed its weapon against the HVU. The purpose of this phase will be to evaluate the impact on the *system* decision making process. As technology increases, so too does our dependence on that technology. The AEGIS weapon system is capable of automatic deployment of weapon systems, given that a threat meets certain predefined parameters. Given this current capability, it is logical to conclude that as the force becomes more and more net-centric, our weapon systems will evolve to encompass this capability. During this phase of the evaluation, human processing becomes less important and relatively small increases to network response times become more significant.

Network traffic will again increase to simulate the escalation of the threat and measurements of latency and throughput recorded for comparison. This phase will terminate once the C-801 has transited inside the minimum engagement range of the carrier’s self-defense weapon systems.

This scenario sets the stage for evaluating the effectiveness of our methodology for developing a bandwidth prioritization scheme. We have sought to capture its impact on not only the human decision makers but also the networked systems involved in the air defense process. The metrics gathered from running this scenario, namely latency and data throughput, will provide an effective yardstick for comparison. The next chapter is dedicated to the development of our model, representing the shipboard networks, which will be placed in this operating environment. This model represents current network capabilities and we can use it to evaluate both prioritization schemes.

THIS PAGE INTENTIONALLY LEFT BLANK

V. QUALITY OF SERVICE MODEL

A key tool for implementing Quality of Service (QoS) management for shipboard IP networks is marking IP packets using the type of service header (ToS) field within the IPv4 header. The Automated Digital Network System (ADNS) uses the first six bits within this octet to mark each packet with a Differentiated Services Code Point (DSCP) (Automated Digital Network System, 2011). These DSCP markings can be used to separate network traffic into class bins which can be used to implement separate controls in off-ship transmission. These traffic bins are General Service (GENSER)—the classification level, i.e., Unclassified, Secret, etc.—ignorant, meaning that even though Secret and Top Secret enclaves are physically separated and encrypted differently, the routing of those packets is done without regard for its GENSER level of classification.

To test the effectiveness of a prioritization scheme in the current Navy environment we need to capture the DSCP process used by ADNS. A stochastic simulation was developed using the *ExtendSim 8* software suite to model this process. Figure 7 provides a simplified rendering of the model's construction and will be used to aid discussion of QoS implementation within ADNS. It is important to note that our simulation focuses on how prioritization schemes impact data throughput and latency within the context of the scenario developed in the previous chapter. We are not modeling the scenario itself, only using it to provide context for the expected data traffic within each phase of an air detect-to-engage (DTE) scenario.

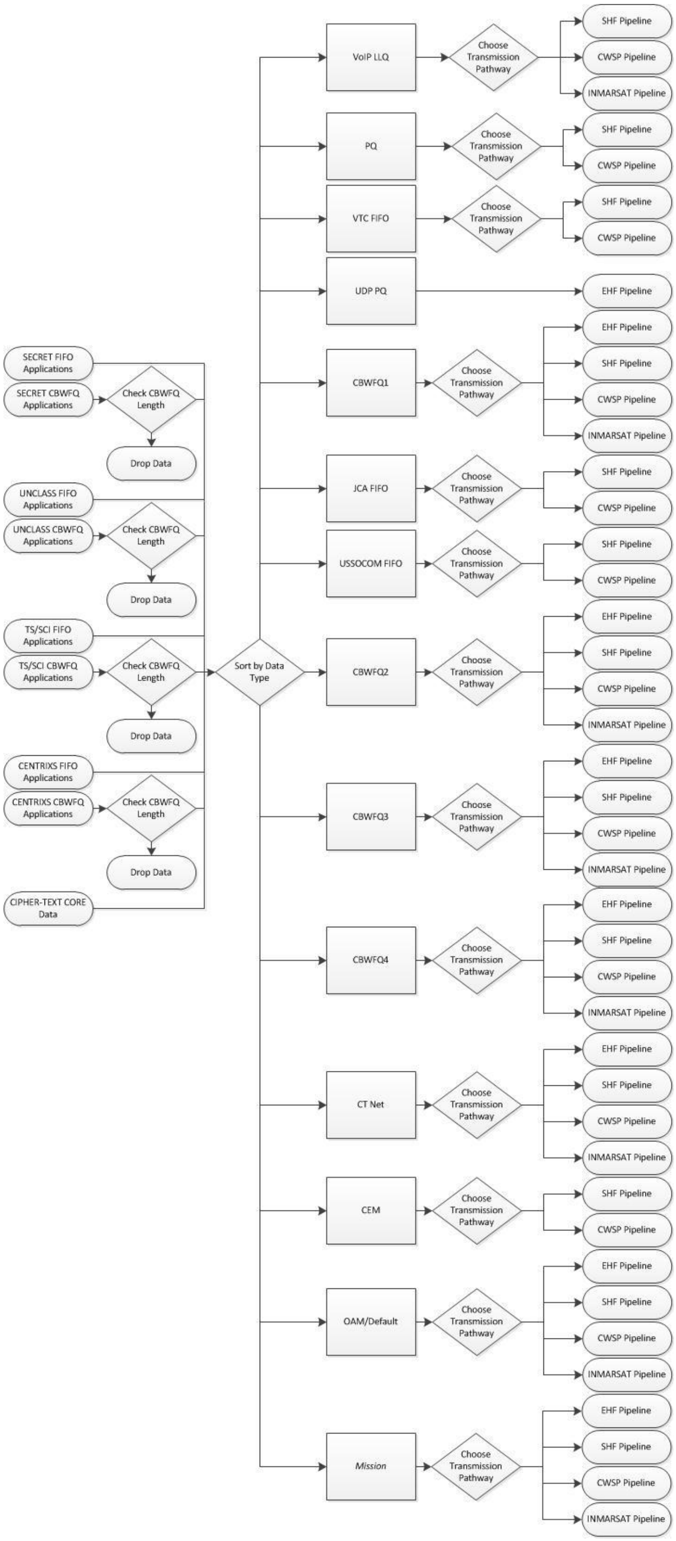

Figure 7. Flow Diagram Representation of *ExtendSim 8* Model

ADNS separates network traffic into five separate Community of Interest (COI) local area networks (LANs). They are SECRET, TS-SCI, UNCLASS, CENTRIXS (coalition), and an additional classification for Cipher Text Core Traffic (Automated Digital Network System, 2011) and are shown on the left side of Figure 7. Each LAN is comprised of various IP-based network applications which are marked using the ToS header and are processed using either First-In, First-Out (FIFO) or Classed-based Weighted Fair Queuing (CBWFQ) queuing doctrine. These applications are listed within the *Traffic Classes, Packet Marking and Priority Processing* documentation provided by the Program Manager, Warfare (PMW) 160 Office. Each of the applications which comprise the COI LANs is represented in our model by a block that creates "packets" with inter-arrival times following a normal distribution. Mean inter-arrival time for each type of application varies depending on the type of service it performs (Table 4).

Application Type	**Mean Inter-arrival Period**	**Standard Deviation**
Video	33 ms	1 ms
VoIP	100 ms	10 ms
Data	200 ms	20 ms
Network Overhead	50 ms	1 ms

Table 4. Application Type Inter-arrival Parameters

These inter-arrival periods were modeled using a normal distribution, bounded by zero on the left side, with a standard deviation as indicated in Table 4. It should be noted that network traffic behavior does not typically adhere to normal distributions but may be classified as "bursty." This means packet inter-arrival periods more closely follow a distribution which may be described as heavy-tailed. This is due in large part to the inherent randomness associated with voice and video applications and the fact that data applications are not used at a constant rate. While utilization of such a distribution would provide for more realistic network behavior, it would introduce a great deal of variability which is not directly related to the purpose of this study and it would have made interpreting the results more complicated. We chose to simplify the analysis by using a normal distribution for the inter-arrival periods. Similarly, each packet produced is assumed to be 1,500 bytes in length; this assumes an absolutely "worst case" scenario in which every application is outputting the maximum amount of data possible. While the two simplifying assumptions introduced in our model would most likely not occur in real-life, they facilitate comparison of prioritization schemes and limit the number of independent variables in the model.

Each of the packets generated in the simulation was marked with a priority based upon the type of information it is carrying. This marking allows for the packet to be routed to one of the fourteen separate queues as shown in Figure 7. ADNS currently specifies thirteen different queue types, based upon network application behavior (Automated Digital Network System, 2011). We introduce a fourteenth *Mission Queue* which is reserved for those applications deemed most relevant to air defense operations. The data from those relevant applications would be marked accordingly and routed to this separate queue. The additional queue is the simplest way to test the proposed prioritization scheme against the existing ADNS scheme. Actual implementation of the prioritization scheme by the Navy might differ based on network configuration and other considerations.

The Voice over IP (VoIP) Low Latency Queues within ADNS receive a fixed amount of bandwidth, dependent upon the entire amount of bandwidth available on a particular transmission channel while the remaining queues share the entire available bandwidth on each channel. All other queues are guaranteed a minimum percentage of bandwidth. There are two divisions of queues within ADNS. For higher capacity pipelines—Super High Frequency (SHF) and Commercial Wideband Satellite Program (CWSP)—queues within the first division are assigned a percentage of the total amount of bandwidth available and that percentage is then parsed out to each application within that group based on an assigned schedule, while queues within the second division are assigned a percentage of bandwidth based on the total amount available. For lower bandwidth pipelines—Extremely High Frequency (EHF) and International Maritime Satellite Program (INMARSAT)—bandwidth percentages assigned are based on the total amount of bandwidth available regardless of grouping.

The model is designed to incorporate only those bandwidth pipelines available to a particular class of ship. Thus, CVNs will be allowed the CWSP, SHF and EHF pipelines, and DDGs and CGs will be allowed the SHF, EHF and INMARSAT pipelines. The model works to balance the load between each of the transmission pipelines available to each queue type as shown in Figure 7. Each bandwidth pipeline will delay the progression of packets by a period equal to the amount of time it would take to transmit that packet. For example, if the EHF pipeline is capable of handling 1.544 Mbps, we will assume one half is reserved for download, leaving us 722 kbps to handle the upload of data. There is no VoIP traffic handled by EHF so we do not need to subtract from it the amount reserved for VoIP. If we wanted to transmit one packet—1,500 bytes—of an application assigned to a queue that has been given 30% of the total bandwidth available for transmission, we would multiply the total bandwidth available by the percentage assigned yielding 231.6 kbps. This means that that this particular queue is capable of handling 231,600 bits of traffic per second. There are 8 bits to a byte, therefore a 1,500 byte Ethernet packet is 12,000 bits in length. Dividing this value by the total transmission speed yields a result of 51.8 ms, or the amount of time the model must delay the packet before transmission. This methodology is applied to each pipeline and used to accurately model the network behavior. This behavior is dynamic, meaning that if a particular queue is not using its bandwidth at that time step, it will give it up. The model checks each time step to see which queues require bandwidth and which do not. It will first subtract from the total amount of bandwidth available that amount which has been assigned to the queues which currently require it and will parse out the remaining bandwidth following the same percentage assignment schedule as outlined in the *Traffic Classes, Packet Marking and Priority Processing* documentation provided by the PMW 160 Office.

ADNS uses two methods for the queuing doctrine applied to each queue. First, applications which are weighted equally within the same queue are handled by a FIFO methodology. Second, applications which are weighted differently, though routed to the same queue, are handled using CBWFQ with Weighted Random Early Detection (WRED). CBWFQ allows for routing of those packets with a higher priority at the expense of those with a lower priority. This is accomplished by randomly dropping lower priority packets, once a queue has reached a pre-determined length.

Beginning at the minimum queue length threshold, packets are dropped following a linear schedule, until the maximum queue length threshold is reached and at which point the maximum percentage of packets dropped is reached. Once the maximum queue length threshold is exceeded, the percentage of packets dropped for an application goes to 100% and all traffic from that application is blocked until the queue length drops below the minimum threshold (Automated Digital Network System, 2011). In our model, this is accomplished by sampling the current queue length for each time step. If the sampled queue length falls within the set boundaries, packets are dropped according to scheduled packet drop probability. Assume for example a queue's minimum length threshold is 20 packets and its maximum queue length threshold is 30 packets. Also assume that at the maximum queue length threshold ten percent of all packets originated by that application type will be dropped. Once this maximum threshold length is exceeded, all traffic will be dropped. Prior to the queue's length reaching 20 packets, all traffic will be transmitted normally. Once the queue length reaches 20 packets, one percent of the packets generated by that application will be dropped; at 21 packets, two percent will be dropped and so on up to the maximum queue length. If a packet is dropped, instead of being routed to the traffic class queue, it is rerouted to a separate activity where it will be delayed the equivalent of one time step. After this delay, it will try the queue length again to see if it falls within the set boundaries or whether it needs to be delayed again.

Within ADNS, this random dropping denies the originating application a receipt acknowledgment by the router and forces the application to retransmit the packet. As more and more packets are randomly dropped, the originating application slows down its rate of transmission to compensate, allowing for higher priority applications to transmit at a faster rate (Automated Digital Network System, 2011). In our model, this metric is captured by measuring the amount of packets that actually were transmitted and comparing that value to the amount of packets that were created. This gives a percentage of actual throughput and will be used as a measure to compare the effectiveness of a given priority scheme as it applies to mission specific applications.

If a queue is not using its assigned bandwidth, the bandwidth will be allocated to the other queues to use until it is needed by the originally assigned queue. This allocation is done proportional to the minimum bandwidth assigned each queue (Automated Digital Network System, 2011). The remaining bandwidth is reserved for traffic bursts and default traffic. The User Datagram Protocol (UDP) queuing is based on application priority, thus all High Priority UDP traffic will be processed before any Medium Priority UDP traffic and so on.

Having modeled the behavior of ADNS, we are now ready to test the effectiveness of each bandwidth management scheme using the scenario we defined in Chapter IV. The following chapter will outline the results of our analysis and provide insights into the data.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RESULTS

A. IMPLEMENTATION OF THE CBCA PRIORITY SCHEME

Using the mapping developed in Chapter III, it is now possible to implement our Capabilities-based Competency Assessment (CBCA) prioritization scheme. In order to capture the CBCA priority in our model, a separate queue was developed and each application type that was relevant to our mission was sent to that queue. This queue was then assigned a percentage of available bandwidth comparable to other queues handling similar data types, the difference being the volume of traffic assigned to our "mission queue."

B. SCENARIO RESULTS

To implement the three separate phases of the scenario, as defined in Chapter IV, and to stress the model, we varied the amount of network traffic generated by each relevant application.

During the first phase, the *Surveillance Phase*, all network traffic remained at default levels. This phase was conducted over a 30 minute period to simulate normal air-defense operations without the presence of a threat. Using the current settings of ADNS INC III, the latency and throughput percentage of our identified systems were recorded for both the carrier (CVN) and cruiser/destroyer (CRUDES) (Table 5). Latency refers to the timeliness of data. By recording latency, we gain an understanding of how long it takes for data to be created, routed and then transmitted. It is important because even if data is 100% complete, but arrives later than it is needed, it is of no use. Throughput refers to how much of the data created is actually transmitted in the time allowed. Acting as the other side of the coin to latency, it does no good for data to arrive instantaneously if it is insufficient to act upon. The latency and throughput results from our ADNS INC III model will act as a baseline for evaluation. Each of the application types that were identified as being relevant to air-defense operations in Chapter III (Table 3) is listed. We recorded the average percent throughput and latency (in milliseconds) for both the carrier (CVN) and the cruiser/destroyer (CRUDES) escorts over a total of 30 runs.

	High Priority Applications		GCCS-M, NETPREC		Time Sync, Chat, COP, HFDF	
	Percent Throughput	Latency	Percent Throughput	Latency	Percent Throughput	Latency
CVN	1.0000	11.122	1.0000	11.207	1.0000	27.778
CRUDES	0.8265	60102.811	0.8284	59262.797	0.3425	110367.857

	Email, CERCIS, OS/BD, PARA126, TDDS		Name Resolution, Encryption, File Transfer, Web, Secure Web		EVCP, Big Brother, ISRT	
	Percent Throughput	Latency	Percent Throughput	Latency	Percent Throughput	Latency
CVN	1.0000	27.917	1.0000	27.879	1.0000	27.894
CRUDES	0.3467	110280.414	0.3445	109629.028	0.3427	110423.471

Table 5. Selected Applications Statistics, Default ADNS Configuration of Systems

The second phase of evaluation is the *Escalation Phase*. During this phase, it is anticipated that the strike group will receive indications of a pending attack on the high value unit (HVU). This phase will last from the time the threat F-4 takes off until it has crossed in the Vital Area (VA) as defined in Chapter IV. As a response to this threat, the strike group commander (BB) will most likely increase his threat warning posture to match the threat being presented. This brings the force to a higher state of readiness in preparation for a possible attack via the air. In order to support this condition, we propose the prioritization scheme shown in Table 6 be implemented, as it brings to the forefront those net-centric systems designed to aid anti-air warfare. By using our process, which links relevant tasks to the operators who must complete them and the systems they must use to do so, we have sought to capture a network prioritization scheme which truly emphasizes air-defense. The bandwidth percentages assigned to each queue were done in such a way as to minimize latency and maximize throughput of those systems we identified as relevant while trying to minimize the impact to those systems we identified as not as important to air-defense operations in Chapter III. It should be noted that the percentages we have assigned are notional and were selected based upon a desired outcome. Our process seeks to simplify the prioritization decision for commanders based on their tactical choices.

Escalation Phase				
	CWSP	SHF	EHF	INMARSAT
Group 1	33%	19%	N/A	N/A
CEM	15%	25%	N/A	N/A
VTC	12%	12%	N/A	N/A
JCA	18%	12%	N/A	N/A
SECRET (CBWFQ1)	12%	7%	27%	17%
UNCLAS (CBWFQ2)	6%	4%	12%	7%
CENTRIXS (CBWFQ3)	6%	4%	12%	4%
SCI (CBWFQ4)	13%	5%	17%	14%
Other				
VoIP (LLQ)	384 kbps	384 kbps	N/A	57 kbps
PQ (FMV)	10%	10%	N/A	N/A
UDP	N/A	N/A	10%	N/A
USSOCOM	24%	24%	N/A	N/A
CT Net (CONTROL)	1%	1%	2%	2%
OAM/Default	11%	25%	5%	41%
Mission	21%	21%	15%	15%

Table 6. CBCA Bandwidth Allocation Scheme – Escalation Phase

The queues listed on the left side of Table 6 are those currently utilized with the Automated Digital Network System (ADNS) (Automated Digital Network System, 2011). We have added the *Mission* queue to the default queue listing and have applied a separate percentage of available bandwidth to it in order to implement our prioritization scheme. The four columns present in Table 6 represent the four transmission paths available to our strike group ships: Commercial Wideband Satellite Program (CWSP)—CVN only, Super High Frequency (SHF), Extremely High Frequency (EHF), and International Maritime Satellite (INMARSAT)—CRUDES only (Automated Digital Network System, 2011). The values in each block represent the percentage of bandwidth available on each transmission path, i.e., column, applied to each queue, i.e., row, with the exception of Voice over Internet Protocol (VoIP) which is a flat amount.

In order to simulate the increase in threat and to further stress the model, the output of our selected applications was effectively doubled. This is based on the assumption that the traffic output of those applications deemed relevant to air defense would increase due to the now present threat and the information being gathered about it. This phase of the scenario was simulated over thirty runs and the average latency and throughput was recorded as shown in Figures 8 through 11. The values along the y-axis in Figures 8 and 10 are milliseconds. The average time to transmit each data type for each prioritization scheme has been recorded for comparison. The values along the y-axis in Figure 9 and 11 are percentages. The average percentage throughput for each data type for each prioritization scheme has been recorded for comparison.

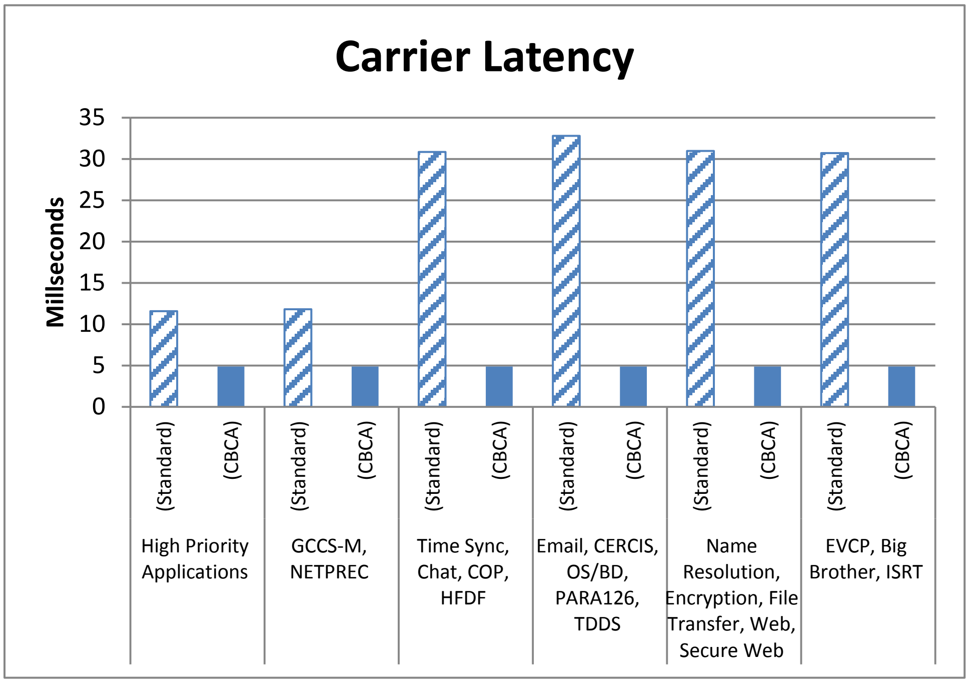

Figure 8. Comparison of Aircraft Carrier Latency in Milliseconds (Escalation Phase)

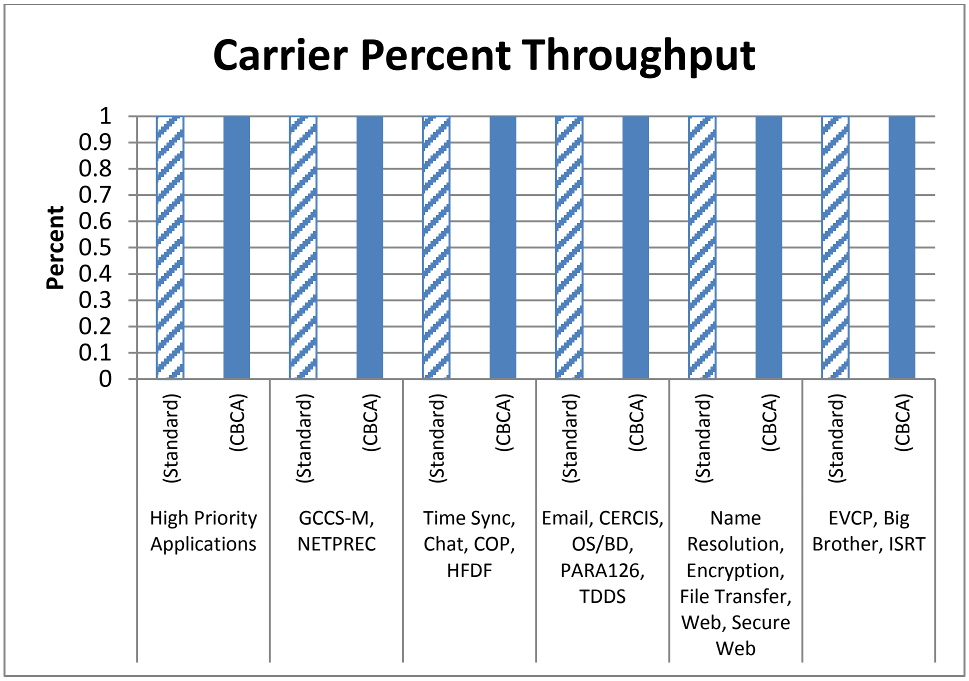

Figure 9. Comparison of Aircraft Carrier Percent Throughput (Escalation Phase)

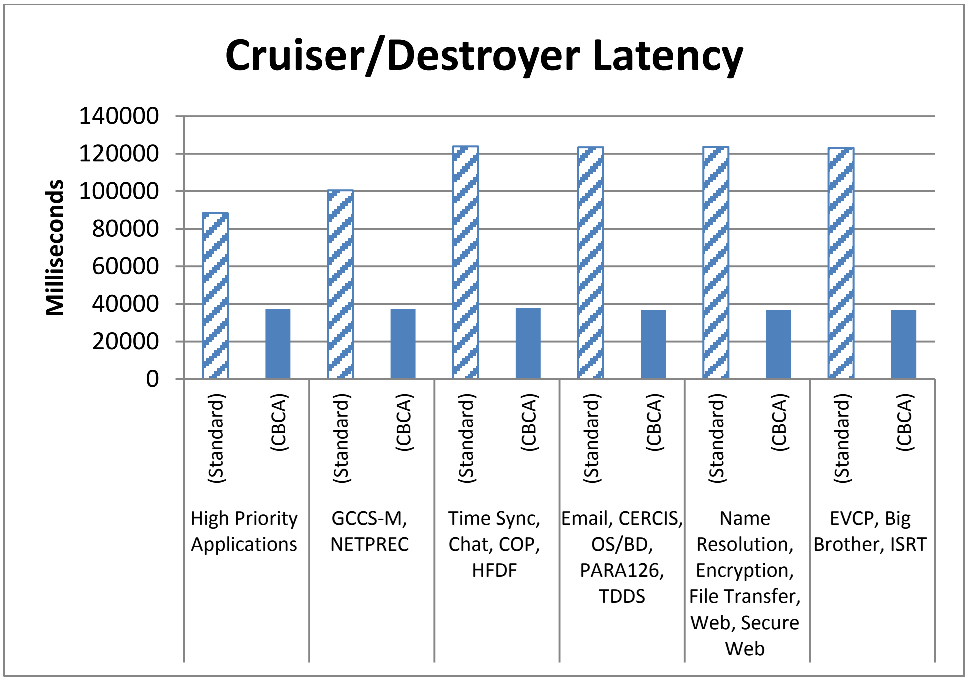

Figure 10. Comparison of Cruiser/Destroyer Latency in Milliseconds (Escalation Phase)

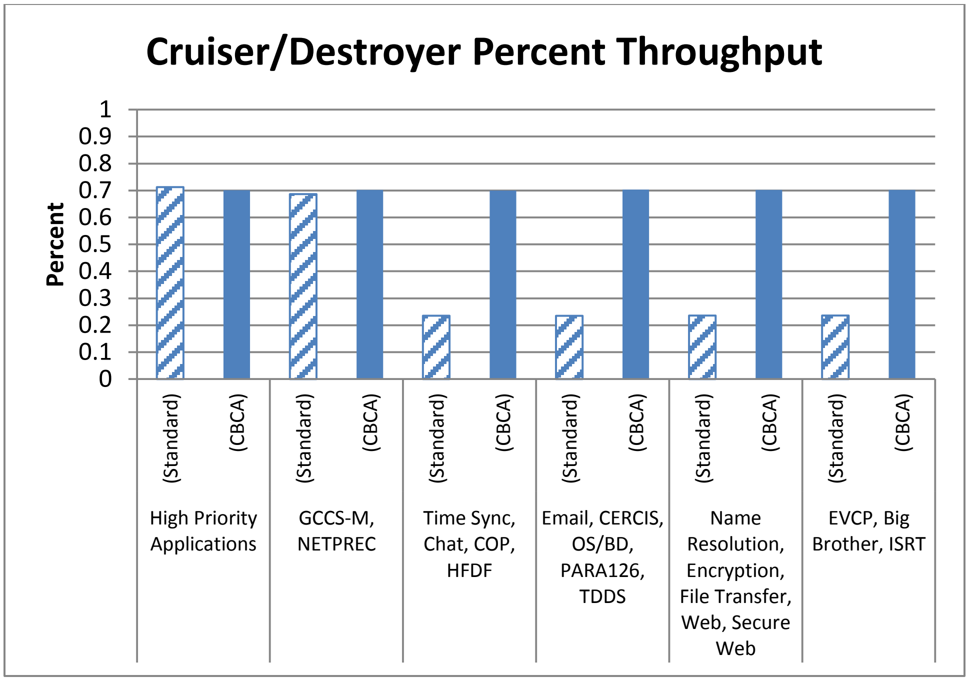

Figure 11. Comparison of Cruiser/Destroyer Percent Throughput (Escalation Phase)

Upon visual inspection, Figures 8 and 10 show marked decreases in the application latency associated with our prioritization schemes—meaning important mission data is being transmitted faster—while Figures 9 and 11 demonstrate at a minimum consistent data throughput and in most cases a significant increase – meaning more important mission data is being transmitted. The difference in the means of the two prioritization schemes was analyzed using an unpaired Student's *t*-test and found to be statistically significant (see Appendix). The simulation indicates a consistent or even increased amount of relevant air-defense information getting through in less time using our prioritization scheme versus the default ADNS prioritization scheme. This is important because information is not only being transmitted faster; it is also being transmitted correctly with greater throughput.

The third phase of evaluation is the *Terminal Phase*. During this phase, it is assumed that the inbound threat will have fired its weapon at the High Value Unit (HVU), prompting BB to further escalate the strike group's readiness posture. This phase will last from the time the threat F-4 has crossed into the VA, fired its weapon (C-801), and the weapon has had sufficient time to traverse the VA and potentially strike its target.

In order to support this condition of readiness, we propose the following prioritization scheme (Table 7) be implemented, as it puts even further emphasis on those net-centric systems designed to aid anti-air warfare. As was done previously, the bandwidth percentages assigned to each queue were done in such a way as to minimize latency and maximize throughput of those systems we deemed relevant while trying to minimize the impact to those systems we deemed not as important to air-defense operations. The bandwidth percentages selected during this phase reflect the increased amount of air-defense relevant network traffic. Again, it should be noted that the percentages we have assigned here were done so to obtain a desired outcome. The actual percentages of bandwidth to be assigned each queue would need to be assigned based upon the commander's priority and intent.

Terminal Phase				
	CWSP	**SHF**	**EHF**	**INMARSAT**
Group 1	30%	15%	N/A	N/A
CEM	15%	25%	N/A	N/A
VTC	12%	12%	N/A	N/A
JCA	18%	12%	N/A	N/A
SECRET (CBWFQ1)	12%	7%	25%	15%
UNCLAS (CBWFQ2)	6%	4%	11%	7%
CENTRIXS (CBWFQ3)	6%	4%	10%	4%
SCI (CBWFQ4)	13%	5%	15%	13%
Other				
VoIP (LLQ)	384 kbps	384 kbps	N/A	57 kbps
PQ (FMV)	10%	10%	N/A	N/A
UDP	N/A	N/A	10%	N/A
USSOCOM	22%	22%	N/A	N/A
CT Net (CONTROL)	1%	1%	2%	2%
OAM/Default	10%	25%	5%	37%
Mission	27%	27%	22%	22%

Table 7. CBCA Bandwidth Allocation Scheme – Terminal Phase

In order to simulate this final phase and to further stress the model, the output of our selected applications was again effectively doubled—now four times the initial value. This is based on the assumption that the traffic output of those applications deemed relevant to air defense would increase due to the now present threat F-4 and the inbound threat missile. The results of this phase of the scenario are presented below (Figures 12—15).

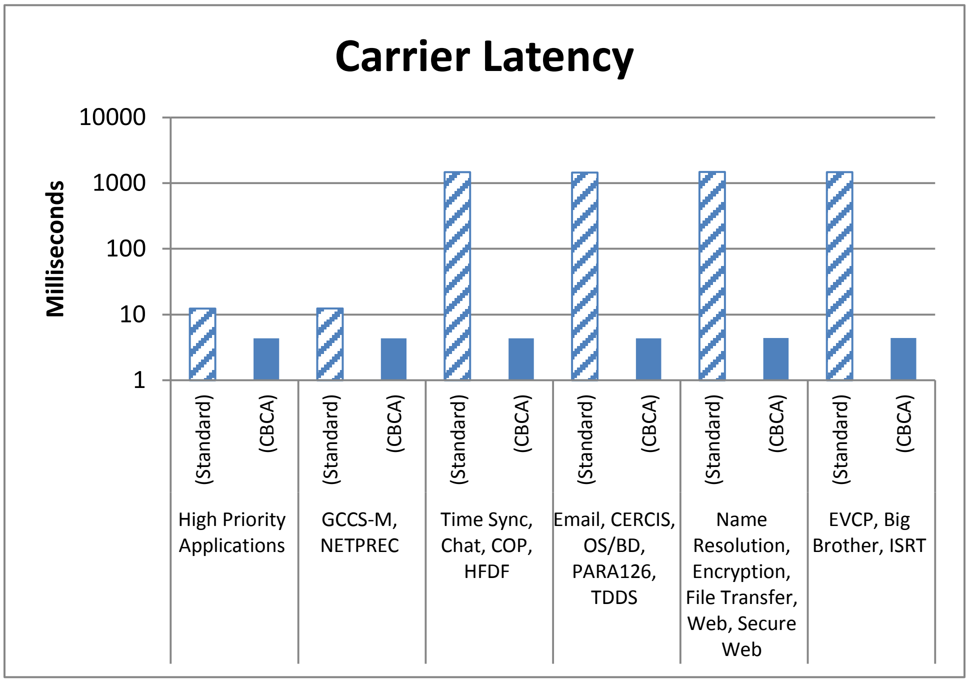

Figure 12. Comparison of Aircraft Carrier Latency in Milliseconds (Terminal Phase)

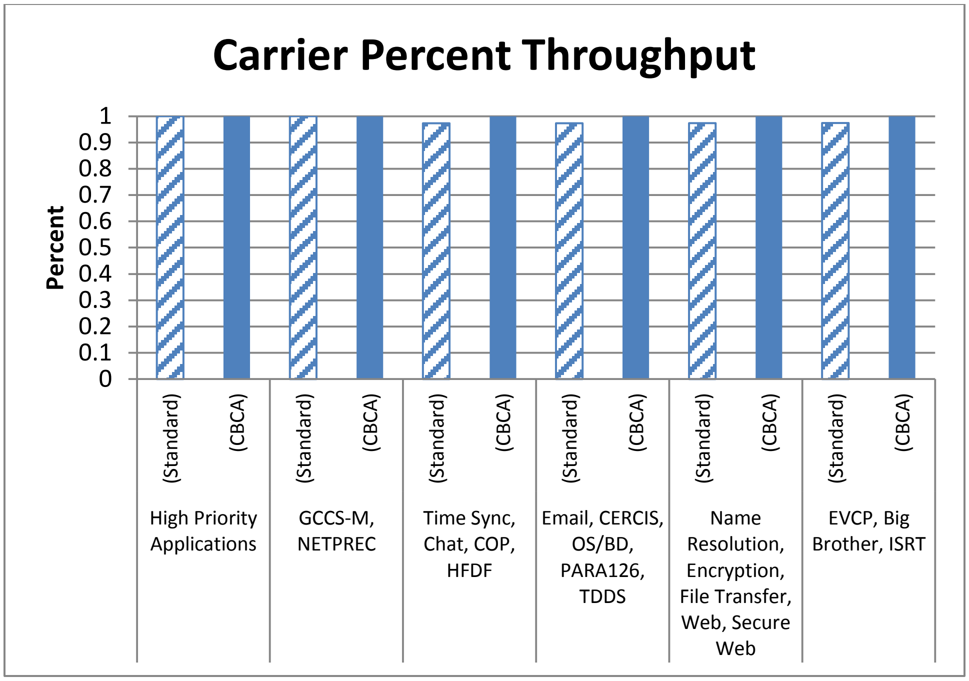

Figure 13. Comparison of Aircraft Carrier Percent Throughput (Terminal Phase)

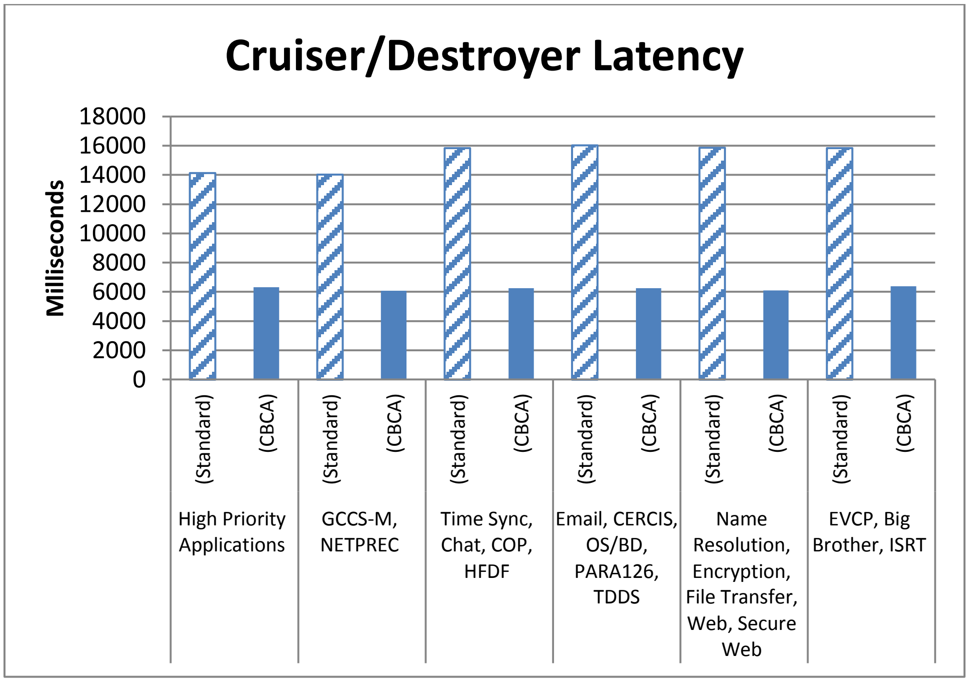

Figure 14. Comparison of Cruiser/Destroyer Latency in Milliseconds (Terminal Phase)

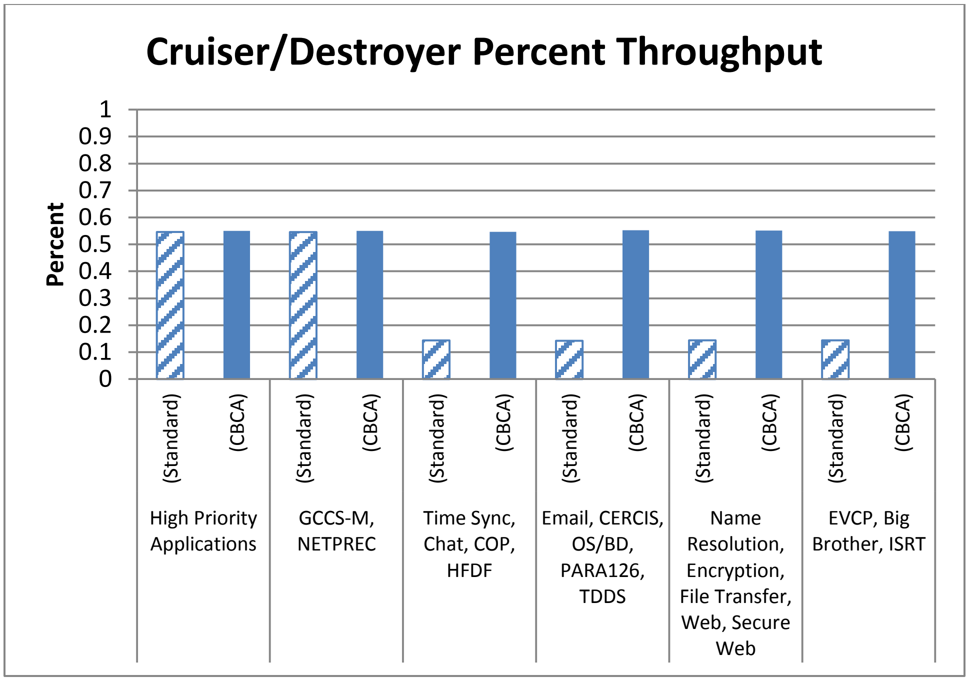

Figure 15. Comparison of Cruiser/Destroyer Percent Throughput (Terminal Phase)

The results shown in Figures 12 and 14 again indicate statistically significant (see Appendix) decreases in data latency associated with our prioritization scheme while Figures 13 and 15 show statistically significant increases in percentage of data throughput—meaning more relevant information is getting through in less time and that information is more complete.

C. IMPACT OF PROPOSED PRIORITIZATION SCHEME

To understand the importance of our prioritization scheme, we must examine the impact of time delays in the context of air defense—a key question is whether or not the differences noted in the previous section are *practically* significant. One of the primary reasons for the selection of this particular warfare area is that time is often at a premium. The C-801 missile was chosen due to its widespread proliferation, but it is by no means the most sophisticated of threats faced by our modern navy; however, it is sufficient to demonstrate the effect of our prioritization scheme.

We will examine the time savings for the CRUDES class ships during the *Terminal Phase* of engagement. From our results, we can see that our prioritization scheme saves on average approximately 9*s* in time delays for our selected applications as compared to the default ADNS prioritization scheme. In order to understand the importance of this time savings, it is beneficial to consider the weapon being used. From Chapter IV, we know the cruising speed of a C-801 is 595 knots. Using the formulas for time distance (Equation 1) we see the actual distance the missile may travel in this allotted time is almost one and a half nautical miles.

$$\begin{gathered} d = vt \\ d = (0.165 nmi/s)(9s) \approx 1.486 nmi \end{gathered} \tag{1}$$

So ultimately, what does the time/distance savings buy us? As the Navy becomes more and more net-centric, our dependency on these systems to "fight the ship"—meaning the actual warfighting for which that ship is designed—will increase. It is reasonable to assume that the end goal of this net-centric approach to warfare is to develop a completely integrated, networked, system-of-systems designed to maximize warfighter capability. To this end, all shipboard systems will be used in the identification and prosecution of hostile targets. The amplifying information these systems provide will be aggregated to provide superior targeting information and reduce our dependency on just one or two sensors to make positive target identifications. Every millisecond we save in the transmission of data results in increased ranges at which may engage hostile targets. This means more time for human decision makers to draw conclusions and more opportunities for us to put ordnance on target.

In their book, *Human Factors in Simple and Complex Systems*, Proctor and Van Zandt (2008) define a reaction-time task as that which requires a person to respond to a stimulus as quickly as possible. They highlight three types of reaction-time tasks: simple reaction time, go-no go reaction time, and choice reaction time (Proctor & Van Zandt, 2008). In simple reaction time tasks, users must react solely at the presence of a stimulus. In go-no go reaction time, users must discern between the presence of one stimulus versus another. The example they provide is responding to the presence of the letter A but no the presence of letter B. In choice reaction time, the user must discern among different responses, each dependent upon the stimulus received. To continue with the previous example, the letter A would prompt one response while the letter B would prompt another. They go on to highlight recent work conducted in continuous information accumulation. According to this behavioral model, human information processing is conducted in parallel, meaning that each stage of the information process is not discrete but that information is rather processed like water moving through a sponge (Proctor & Van Zandt, 2008). This model suggests that as information is received, the brain may begin processing of that information, prompting a response before the actual response is made. This prompting may lead to errors as operators attempt to respond as quickly as possible to the given stimuli. They may reach the wrong conclusion if their minimum processing threshold is set too low in order to decrease their response time. Proctor and Van Zandt argue that this model is the only one which explains the relationship between human response time and accuracy. They cite as observation that the fastest possible human reaction to simple reaction time tasks is 150 ms for visual stimuli. This reaction time slows linearly, following a $\log_2$ scale, with the number of possible stimuli and responses available to the operator.

If we assume the previously described mean reaction time, we see that the time savings described in this paper are within the threshold of human reaction. This is critical as it allows for an actual physical response by a human operator. The more the latency of our selected data is reduced, the more time the human decision maker has to react to the visual stimulus. This impact is even more drastic as we consider the near instantaneous reaction time of automated systems. For example, assume a human operator must choose between ten separate alternative responses to the given stimuli. According to the research conducted by William Hick, reaction time increases as a logarithmic function of the number of stimuli (Proctor & Van Zandt, 2008) (Equation 2):

$$\begin{aligned} &\text{Reaction time (s)} = \mathrm{Log}_2 n \\ &\text{Number of stimuli, } n = 10 \\ &\text{Reaction time (s)} = \mathrm{Log}_2 10 = 3.322s \end{aligned} \qquad (2)$$

This means that more than 3 seconds will elapse before a reasonable human response may be expected. Machines are not limited by this delay and the response to stimuli will be nearly instantaneous—assuming some reasonable threshold of stimuli—with the only delay being the time it takes for information to reach the computer system. While at some point, the amount of processing required would exceed the capacity of a computer, the amount of information present in an air defense environment is insufficient to overwhelm current computer systems. Again using the formulas for time distance (Equation 3):

$$\begin{aligned} d &= vt \\ d &= (0.165 nmi/s)(3.322s) = 0.548 nmi \end{aligned} \tag{3}$$

We see that by removing the human decision maker from the equation we can expect marked increases in the distance at which a hostile target may be engaged.

Additionally, the C-801 was chosen as the hostile target in this scenario due to its wide proliferation, not necessarily its capability. More and more sophisticated anti-ship missiles are being fielded with cruising velocities exceeding multiples of Mach 1. Given an autonomous response capability, milliseconds saved in transmission time can directly translate to whether an enemy target may be destroyed in the allotted time or if it will strike its intended target.

In this chapter we have presented results of our network simulations for an air detect-to-engage (DTE) sequence comparing default ADNS network prioritization and our CBCA-based methodology for network prioritization. The results of our analysis indicated marked network performance increases using our CBCA-based process. Our evaluation took place over three separate phases of an air detect-to-engage (DTE) in which we sought to simulate ADNS network response to an increasing threat. During the first phase (Surveillance Phase) we established a base network performance measure for ADNS which was used to gauge the effectiveness of existing network prioritization. The next two phases (Escalation Phase and Terminal Phase) were dedicated to examining the impact of our prioritization methodology on the network response to the emerging threat and comparing it to the current prioritization methodology implemented within ADNS. A summary of these results (Table 8), in which the average latency (in milliseconds) and percent throughput for all network applications were recorded and compared, has been included for clarification purposes.

	Escalation Phase		Terminal Phase	
	CVN	**CRUDES**	**CVN**	**CRUDES**
Average Latency (Standard)	24.772	113811.943	981.396	15291.243
Average Latency (CBCA)	4.863	37056.427	4.386	7624.121
Percent Reduction in Latency	*-80.37%*	*-67.44%*	*-99.55%*	*-50.14%*
Average Percent Throughput (Standard)	99.998%	39.032%	98.234%	27.771%
Average Percent Throughput (CBCA)	99.999%	70.209%	99.995%	54.990%
Percent Increase in Throughput	*0.0009%*	*14.6147%*	*1.7553%*	*4.4879%*

Table 8. Comparison of Average Latency and Throughput for Standard and CBCA Network Prioritization

It should be noted that the values shown in Table 8 are merely averages of all air defense network applications. The individual values for each application type and evidence of statistical significance are presented in the Appedix. Our results indicated consistent reduction in network latency and increased throughput for network applications we identified as being relevant to air defense operations when using our prioritization methodology. These network improvements translate directly to improved warfighting capacity and information dominance.

VII. CONCLUSION

A. SUMMARY

This document sought to answer two questions:

> 1) What is the feasibility of developing a bandwidth utilization priority scheme based upon identified tasks and information required by warfighters to conduct military operations within a hostile environment?
>
> 2) How will this systematic allocation process, based upon warfighter information needs and dynamically tailored for various threats, affect data latency and information throughput?

We have demonstrated a process which seeks to properly align system prioritization with operator needs based upon mission tasking. Such a methodology works by linking operational tasking to warfighters, working within a command infrastructure, and identifying those systems used by those warfighters to accomplish said tasking. Our work may be seen as a guideline for the development of network prioritization schemes which seek to optimize Navy networks for combat and are in keeping with the philosophy of net-centric warfare (NCW). Ideally, strike group commanders would leverage our approach to facilitate communication between the technical and tactical personnel under their command and develop an intimate understanding of their networks as true weapon systems. Such an understanding allows for commanders to optimize the network assets at their disposal and bring to the forefront those network systems relevant to the mission-at-hand.

The information we have presented in this study makes the case for competency-based network prioritization based on the needs of the warfighter. This is not to say that network application characteristics should not be taken into account, only that they should not be the only force which drives network prioritization.

Through modeling and simulation, we have demonstrated the effectiveness of our bandwidth prioritization on reducing relevant data latency and increasing information throughput. Doing so allows for longer dwell times for human and machine responses to the threat environment and translates into information dominance. Our process provides a tool for commanders to develop pre-planned responses for network prioritization, just as they would for any other weapon system at their disposal.

B. FUTURE RESEARCH

We believe it would be highly beneficial to expand our network model. We have shown the effectiveness of our prioritization scheme in processing information for a single ship, but a model which encompasses not only the relationships of onboard systems, but the relationships between ships within the strike group and the Internet at large would be valuable. Our model sought to mimic the stochastic processes inherent to network behavior; however a higher resolution model which incorporates Department of Defense (DoD) specific applications may be of great use. Additionally we have made several simplifying assumptions, namely in the assumption of normality in the underlying distribution of packet inter-arrival periods as well as the size of all network packets. In order to truly model network behavior, more realistic assumptions would need to be made. True packet inter-arrival rates conform to a distribution which is more heavy-tailed and there is a great deal of variability associated with packet size. The inherent "burstiness" of network traffic introduces a great deal of variability and increases the risk of critical information not being received in time. In order to determine the effectiveness of our prioritization scheme in limiting this risk, evaluations of our model using these type of assumptions will have to be performed.

Additional research should be conducted on the implementation of identified processes and technologies for dynamic Quality of Service (QoS) within the DoD environment. While technological advances have been made in this area of research, further efforts will be required before solutions may be implemented for warfighter use. Real-time simulation of dynamic bandwidth allocation, utilizing some of the identified processes, in a real-world scenario would no doubt provide much insight into the applicability of new technologies in NCW.

Finally, our process was designed to provide an outline for how a capability-based network prioritization scheme should be developed. The example we have provided serves only to demonstrate our method and should not be taken at face value. Any prioritization scheme that is truly tailored for warfighter optimization should be originated and vetted by the technical and tactical experts it is designed to augment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX

This appendix contains the results of the independent two-sample, single-tailed Student *t*-tests conducted to confirm statistical significance between recorded results for each phase of our model. The mean latency and percent throughput, and the associated standard deviations (based on 30 runs), were recorded for both the default ADNS settings as well as our CBCA Recommended Settings as presented in Chapter VI, Tables 6 and 7 (Tables 9 and 10).

CARRIER					
		LATENCY		PERCENT THROUGHPUT	
STANDARD					
APPLICATION NAME	PHASE	AVERAGE VALUE (ms)	VARIANCE (ms^2)	AVERAGE VALUE	VARIANCE
High Priority Applications	Escalation	11.563	0.049	1.000	0.000
	Terminal	12.340	0.199	1.000	0.000
GCCS-M, NETPREC	Escalation	11.795	0.196	1.000	0.000
	Terminal	12.382	0.114	1.000	0.000
Time Sync, Chat, Cop, HFDF	Escalation	30.834	0.760	1.000	0.000
	Terminal	1468.693	69685.262	0.973	0.000
Email, CERCIS, OS/BD, PARA126, TDDS	Escalation	32.783	1.419	1.000	0.000
	Terminal	1446.886	73660.365	0.973	0.000
Name Resolution, Encryption, File Transfer, Web, Secure Web	Escalation	30.956	0.556	1.000	0.000
	Terminal	1478.850	87447.835	0.974	0.000
EVCP, Big Brother, ISRT	Escalation	30.698	0.444	1.000	0.000
	Terminal	1469.226	90779.519	0.974	0.000
CBCA					
High Priority Applications	Escalation	4.863	0.008	1.000	0.000
	Terminal	4.381	0.011	1.000	0.000
GCCS-M, NETPREC	Escalation	4.863	0.007	1.000	0.000
	Terminal	4.370	0.011	1.000	0.000
Time Sync, Chat, Cop, HFDF	Escalation	4.869	0.008	1.000	0.000
	Terminal	4.371	0.015	1.000	0.000
Email, CERCIS, OS/BD, PARA126, TDDS	Escalation	4.855	0.008	1.000	0.000
	Terminal	4.369	0.010	1.000	0.000
Name Resolution, Encryption, File Transfer, Web, Secure Web	Escalation	4.868	0.009	1.000	0.000
	Terminal	4.400	0.015	1.000	0.000
EVCP, Big Brother, ISRT	Escalation	4.863	0.008	1.000	0.000
	Terminal	4.423	0.010	1.000	0.000

Table 9. Comparison of Average Latency and Percent Throughput for Selected Applications, Standard ADNS Settings vs. CBCA Settings (CARRIER).

CRUDES					
		LATENCY		PERCENT THROUGHPUT	
STANDARD					
APPLICATION NAME	PHASE	AVERAGE VALUE (ms)	VARIANCE (ms^2)	AVERAGE VALUE	VARIANCE
High Priority Applications	Escalation	88310.839	4603663.159	0.713	0.000
	Terminal	14136.054	198908.455	0.546	0.000
GCCS-M, NETPREC	Escalation	100479.722	8851334.897	0.687	0.000
	Terminal	14030.140	221936.916	0.546	0.000
Time Sync, Chat, Cop, HFDF	Escalation	123889.406	5005164.206	0.235	0.000
	Terminal	15840.933	544548.019	0.144	0.000
Email, CERCIS, OS/BD, PARA126, TDDS	Escalation	123398.811	3793578.564	0.235	0.000
	Terminal	16030.951	585599.966	0.142	0.000
Name Resolution, Encryption, File Transfer, Web, Secure Web	Escalation	123693.960	5802303.837	0.236	0.000
	Terminal	15867.789	527594.057	0.144	0.000
EVCP, Big Brother, ISRT	Escalation	123098.919	5670824.102	0.236	0.000
	Terminal	15841.591	670709.971	0.144	0.000
CBCA					
High Priority Applications	Escalation	37217.901	2958803.686	0.701	0.000
	Terminal	6306.229	374775.609	0.550	0.000
GCCS-M, NETPREC	Escalation	37140.539	3293858.849	0.702	0.000
	Terminal	6067.029	447836.757	0.551	0.000
Time Sync, Chat, Cop, HFDF	Escalation	37827.175	2394056.060	0.700	0.000
	Terminal	6250.266	365535.722	0.546	0.000
Email, CERCIS, OS/BD, PARA126, TDDS	Escalation	36629.429	3646216.929	0.704	0.000
	Terminal	6240.466	288647.262	0.552	0.000
Name Resolution, Encryption, File Transfer, Web, Secure Web	Escalation	36915.146	3335255.969	0.703	0.000
	Terminal	6095.606	251524.111	0.551	0.000
EVCP, Big Brother, ISRT	Escalation	36608.370	2895832.627	0.702	0.000
	Terminal	6378.301	326772.170	0.549	0.000

Table 10. Comparison of Average Latency and Percent Throughput for Selected Applications, Standard ADNS Settings vs. CBCA Settings (CRUDES).

These results may be used to conduct statistical analysis. The first step in the determination of the statistical significance of our results is the development of the correct hypothesis test for comparison of the mean values of our model results. There are two parts to hypothesis testing, the null hypothesis (H_o)—which in this case will be the assumption that the mean values of our test populations are not statistically different – and the alternative hypothesis (H_a)—which in this case will be the assumption that the mean values of our test populations are statistically different.

The independent two-sample Student *t*-test is defined as follows:

$$t_{value} = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{1}{2}(s_{x1}^2 + s_{x2}^2)} \cdot \sqrt{\frac{2}{n}}} = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{(s_{x1}^2 + s_{x2}^2)}{n}}} \tag{4}$$

Where $\bar{X}_1$ is equal to the mean of the first sample and $\bar{X}_2$ is equal to the mean of the second sample, s_{x1}^2 is equal to the variance of the first sample and s_{x2}^2 is equal to the variance of the second sample and *n* is equal to the size of the both the first and second samples (Hayter, 2007). This test assumes that both samples consist of the same number of observations, in our case 30, and that the distributions of both populations have an equal variance. The resulting *t*-value (t_{obsv}) is then compared to known critical *t*-values (t_{crit}) from a *t*-distribution table and, depending upon the results, there will either be sufficient evidence to reject H_o—meaning the means of our populations are statistically different – or there is insufficient evidence to reject H_o—meaning we must conclude that the mean values of the two populations are not statistically different.

When looking up the t_{crit} for the given conditions, one must determine the applicable degrees of freedom (ν) and assume a threshold of statistical significance (α). In this test, ν is defined as $2n-2$ where *n* is the number of observations in each group, resulting in a value of 58. Typically in hypothesis testing of this type, an α value of 0.05 is used. A single-tailed *t*-distribution is used when one is trying to prove that a population's mean value is either higher (right-side of the distribution) or lower (left-side of the distribution) than another population's mean, not just different. Because we are only interested in results which will confirm decreases in data latency and increases in information throughput, a single-tailed test was used to compare the means of each population. Using the defined parameters for ν and α yields a t_{crit} of 1.672. This value is positive when using the right-side of the distribution and negative when using the left-side of the distribution. If the absolute value of t_{obsv} is greater than the absolute value of t_{crit} then there is sufficient evidence to reject H_o.

For our purposes, we will assume the first population consists of the results from the default ADNS settings and the second population consists of the results from our recommended CBCA settings. Therefore, when testing for the statistical significance of data latency, our alternative hypothesis will be that mean value of the first population is greater than that of the second population, and when testing for the statistical significance of percent throughput, our alternative hypothesis will be that the mean value of the first population is less than that of the second population. The null hypothesis for both comparisons of latency and percent throughput will be that the means of the populations are not different. The results of our hypothesis testing are presented below (Tables 11—14).

CARRIER LATENCY HYPOTHESIS TEST						
APPLICATION NAME	**PHASE**	H_o	H_a	t_{obsv}	t_{crit}	**Reject** H_o
High Priority Applications	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	153.023	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	95.038	1.672	Yes
GCCS-M, NETPREC	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	84.214	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	123.864	1.672	Yes
Time Sync, Chat, Cop, HFDF	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	162.315	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	30.383	1.672	Yes
Email, CERCIS, OS/BD, PARA126,	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	128.046	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	29.111	1.672	Yes
Name Resolution, Encryption, File	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	190.009	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	27.310	1.672	Yes
EVCP, Big Brother, ISRT	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	210.461	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	26.628	1.672	Yes

Table 11. CARRIER Latency Hypothesis Test Results

CRUDES LATENCY HYPOTHESIS TEST						
APPLICATION NAME	**PHASE**	H_o	H_a	t_{obsv}	t_{crit}	**Reject** H_o
High Priority Applications	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	101.763	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	56.621	1.672	Yes
GCCS-M, NETPREC	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	99.548	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	53.294	1.672	Yes
Time Sync, Chat, Cop, HFDF	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	173.293	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	55.064	1.672	Yes
Email, CERCIS, OS/BD, PARA126,	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	174.240	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	57.352	1.672	Yes
Name Resolution, Encryption, File	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	157.239	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	60.639	1.672	Yes
EVCP, Big Brother, ISRT	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	161.854	1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 > \bar{X}_2$	51.898	1.672	Yes

Table 12. CRUDES Latency Hypothesis Test Results

CARRIER THROUGHPUT HYPOTHESIS TEST						
APPLICATION NAME	**PHASE**	H_o	H_a	t_{obsv}	t_{crit}	**Reject** H_o
High Priority Applications	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	1.015	-1.672	No
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-1.172	-1.672	No
GCCS-M, NETPREC	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	0.448	-1.672	No
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-0.685	-1.672	No
Time Sync, Chat, Cop, HFDF	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-3.247	-1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-21.000	-1.672	Yes
Email, CERCIS, OS/BD, PARA126,	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-1.206	-1.672	No
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-22.156	-1.672	Yes
Name Resolution, Encryption, File	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-3.808	-1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-21.693	-1.672	Yes
EVCP, Big Brother, ISRT	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-2.424	-1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-22.553	-1.672	Yes

Table 13. CARRIER Throughput Hypothesis Test Results

CRUDES THROUGHPUT HYPOTHESIS TEST						
APPLICATION NAME	**PHASE**	H_o	H_a	t_{obsv}	t_{crit}	**Reject** H_o
High Priority Applications	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	8.063	-1.672	No
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-1.514	-1.672	No
GCCS-M, NETPREC	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-9.655	-1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-1.472	-1.672	No
Time Sync, Chat, Cop, HFDF	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-427.218	-1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-158.074	-1.672	Yes
Email, CERCIS, OS/BD, PARA126,	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-445.372	-1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-158.543	-1.672	Yes
Name Resolution, Encryption, File	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-387.054	-1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-169.129	-1.672	Yes
EVCP, Big Brother, ISRT	Escalation	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-373.809	-1.672	Yes
	Terminal	$\bar{X}_1 = \bar{X}_2$	$\bar{X}_1 < \bar{X}_2$	-160.739	-1.672	Yes

Table 14. CRUDES Throughput Hypothesis Test Results

From these results, it is evident that there is a statistically significant decrease in the average latency associated with each of the selected applications using our prioritization methodology as compared to default ADNS settings. These results also indicate statistically significant increases in throughput using our prioritization scheme for most applications; however there is no significant difference for some applications. We note decreases in percent throughput for the *High Priority Applications* data types for both the CARRIER and CRUDES type ships during the *Escalation Phase* as well as *GCCS-M, NETPREC* data types for the CARRIER during the *Escalation Phase* when using our prioritization scheme. This decrease in percent throughput is offset by marked decreases in associated latency which should be taken into consideration when implementing our process for network prioritization.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Automated Digital Network System. (2011). *QoS traffic classes, packet marking and priority processing, rev 10.* San Diego, CA: PEO C4I.

Bartolomasi, P., Buckman, T., Campbell, A., Grainger, J., Mahaffey, J., Marchand, R., Kruidhof, O., Shawcross, C., & Veum, K., (2005). *NATO network enabled capability feasibility study v. 2.0.* Brussels, Belgium: NATO Consulatation, Command and Control Agency

Chief of Naval Operations, Commandant, United States Marine Corp, Commandant, United States Coast Guard. (2007). *Universal naval task list (UNTL).* Washington, DC: Chief of Naval Operations, Commandant of the Marine Corps, and Headquarters, United States Coast Guard.

Consolidated networks and enterprise services (CANES). (n.d.). Retrieved January 13, 2012, from SPAWAR: http://www.public.navy.mil/spawar/productsServices/Pages/ConsolidatedAfloatNetworksandEnterpriseServicesCANES.aspx

DoD. (2007). *DoD architecture framework version 1.5.* Washington, DC: Author.

DoD. (2009). *DoD architecture framework version 2.0.* Washington, DC: Author.

F-4 Phantoms phabulous 40th. (n.d.). Retrieved October 29, 2011, from Boeing: www.boeing.com/defense-space/military/f4/index.htm

Goure, D. (2011, January 6). *The essence of American global power is the carrier strike group*. Retrieved August 19, 2011, from Defence Professionals: http://www.defpro.com/news/details/21002/?SID=9fb68405914d788eddbb41f300c36efc

Hayter, A. J. (2007). *Probability and statistics for engineers and scientists*, 3rd ed. Bemont: Thomson Higher Education.

Hwang, W. S., & Tseng, P. C. (2005). A QoS-aware residential gateway with bandwidth management. *IEEE transactions on consumer electronics*, xx, 840–848.

Kashihara, S., & Tsurusawa, M. (2010). Dynamic bandwidth management system using IP flow analysis for the QoS-assured network. *Global telecommunications conference*, 1–5.

Loyall, J. P., Gillen, M., Paulos, A., Bunch, L., Carvalho, M., Edmondson, J., et al. (2010). Dynamic policy-driven quality of service in service-oriented systems. *13th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing,* 1–9.

Lund, K., Eggen, A., Hadzic, D., Hafsøe, T., & Johnsen, F. T. (2007, October). Using web services to realize service oriented architecture in military communication networks. *IEEE communications magazine,* 47–53.

Mahan, A. T. (1890). *The influence of sea power on history.* Boston: Little, Brown and Company.

McDonell Douglas F-4D. (2009, Novemebr 2). Retrieved October 29, 2011, from National Museum of the U.S. Air Force: www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=2276

Morua, M. L. (2000, March 21). *The carrier battle group force: An operator's perspective.* Retrieved August 19, 2011, from Defense Technical Information Center: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA376409&Location=U2&doc=GetTRDoc.pdf

Naval transformation roadmap. (2003). Retrieved July 6, 2011, from Navy.mil: www.navy.mil/navydata/transformation/trans-toc.html

Office of Force Transformation. (2005). *Implementation of network-centric warfare.* Washington, DC: Author.

Office of the President of the United States. (2010). *National security strategy*. Washington, DC: The White House.

PEO C4I. (2010). *PEO master plan version 4.0.* San Diego: Program Executive Officer, Command, Control, Communications, Computers and Intelligence.

PEO C4I. (2011). *PEO master plan version 5.0.* San Diego: Program Executive Officer, Command, Control, Communications, Computers and Intelligence.

Pike, J. (2011, July 11). *C-801 YJ-1 / YJ-8 (Eagle Strike) / YJ-83 / CSS-N-4 SARDINE*. Retrieved October 29, 2011, from GlobalSecurity.org: www.globalsecurity.org/military/world/china/c-801.htm

Polmar, N. (2005). *The Naval Institute guide to the ships and aircraft of the U.S. fleet.* Annapolis: U.S. Naval Institute.

Proctor, R. W., & Van Zandt, T. (2008). *Human factors in simple and complex systems.* Boca Raton, FL: CRC Press.

Rambo, M. (2011, September). ADNS QoS. Lecture conducted from PEO C4I, San Diego.

Ronga, L. S., Pecorella, T., Re, E. D., & Fantacci, R. (2003). A gateway architecture for IP satellite networks with dynamic resource mangement and DiffServ QoS provision. *International journal of satellite communications and networking*, 351–366.

Salsano, S., & Veltri, L. (2002). QoS control by means of COPS to support SIP-based applications. *IEEE network*, 27–33.

Suttie, R. D., & Potter, N. J. (2008). *Capability based competency assessment (CBCA).* Newport: United States Naval War College.

Szigeti, T., & Hattingh, C. (2004). *End-to-end QoS network design: Quality of service in LANs, WANs, and VPNs.* Indianapolis: Cisco Press.

United States Navy. (n.d.). Retrieved April 4, 2012, from The Carrier Strike Group: http://www.navy.mil/navydata/ships/carriers/powerhouse/cvbg.asp

Vego, M. N. (2007). *Joint operational warfare: Theory and practice.* Newport: United States Naval War College.

Wang, G., Chen, A., Wang, C., Fung, C., & Uczekaj, S. (2004). Integrated quality of service (QoS) management in service-oriented enterprise architectures. *8th IEEE intl enterprise distributed object computing conf.* Monterey, CA: IEEE Computer Society.

Welford, W. T. (1980). *Reaction times.* London: Academic Press.

White, P. P. (1997). RSVP and integrated services in the Internet: A tutorial. *IEEE communications magazine*, 100–106.

Xiao, X., & Ni, L. M. (1999). Internet QoS: A big picture. *IEEE network*, 8–18.

Zhao, H., Niu, W., Qin, Y., Ci, S., Tang, H., & Lin, T. (2012). Traffic load-based dynamic bandwidth allocation for balancing the packet loss in DiffServ network. *2012 IEEE/ACIS 11th international conference on computer and information science*, 99–104.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, VA

2. Dudley Knox Library
Naval Postgraduate School
Monterey, CA

3. Dr. Diana M. Angelis
Naval Postgraduate School
Monterey, CA

4. Gregory Miller
Naval Postgraduate School
Monterey, CA

5. Dr. Rachel Goshorn
Naval Postgraduate School
Monterey, CA

6. Dr. Robert Parker (CAPT, USN Ret.)
SPAWAR PEO C4I APEO for S&T, SPAWAR CTO
San Diego, CA

7. RDML Jerry Burroughs
SPAWAR PEO C4I
San Diego, CA

8. Pat Sullivan
SPAWAR PEO C4I Executive Director
San Diego, CA

9. CAPT John Pope
SPAWAR, Fleet Readiness Directorate
San Diego, CA

10. Jerry Almazan
SPAWAR PEO C4I, PMW 120
San Diego, CA

11. Delores Washburn
SPAWAR PEO C4I, PMW 160
San Diego, CA

12. Alexander Vasel
SPAWAR PEO C4I, PMW 160
San Diego, CA

13. Charles Suggs
SPAWAR PEO C4I, DPEO Technical Direction & Program Integration
San Deigo, CA

14. Dr. Kurt Kiscko
SPAWAR PEO C4I, PMW 170
San Diego, CA

15. CAPT Joe Beel
Commanding Officer, SPAWAR Systems Center Pacific
San Diego, CA

16. CAPT Bryan Lopez
Executive Officer, SPAWAR Systems Center Pacific
San Diego, CA

17. Ruth Youngs Lew
SPAWAR PEO C4I, PMW 790
San Deigo, CA